Rada
Európskej únie

V Bruseli 26. novembra 2021
(OR. en)

14337/21

Medziinštitucionálny spis:
2020/0359(COD)

CODEC 1541
CSC 416
CSCI 147
CYBER 312
DATAPROTECT 269
JAI 1295
MI 891
TELECOM 435

POZNÁMKA

Od:	Generálny sekretariát Rady
Komu:	Rada
Č. predch. dok.:	9583/2/21, 11724/21
Č. dok. Kom.:	14150/20
Predmet:	Návrh smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa zrušuje smernica 2016/1148 – *všeobecné smerovanie*

I. ÚVOD

1. Komisia 16. decembra 2020 prijala návrh smernice o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii (ďalej len „revidovaná smernica NIS“ alebo „NIS 2“)[1] s cieľom nahradiť súčasnú smernicu o bezpečnosti sietí a informačných systémov (ďalej len „smernica NIS“)[2].

[1] Návrh smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii a o zrušení smernice (EÚ) 2016/1148.

[2] Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii.

Návrh bol jedným z opatrení stanovených v Stratégii kybernetickej bezpečnosti EÚ v digitálnej dekáde[3], ktorých cieľom je zabezpečiť, aby občania a podniky mohli využívať dôveryhodné digitálne technológie.

2. Tento návrh sa zakladá na článku 114 Zmluvy o fungovaní Európskej únie (ZFEÚ) a jeho cieľom je ďalej zlepšovať odolnosť verejných a súkromných subjektov, príslušných orgánov a Únie ako celku a ich schopnosť reagovať na incidenty.

3. V Európskom parlamente je gestorským výborom pre návrh Výbor pre priemysel, výskum a energetiku (ITRE). Výbor ITRE prijal spravodajcovu správu 28. októbra 2021.

4. Európsky hospodársky a sociálny výbor zaujal stanovisko 28. apríla 2021.

5. Výbor stálych predstaviteľov sa 3. februára 2021 rozhodol tento návrh prekonzultovať s Európskym výborom regiónov[4]. Európsky výbor regiónov zatiaľ stanovisko nezaujal.

6. Európsky dozorný úradník pre ochranu údajov zaujal stanovisko 11. marca 2021[5].

7. Rada prijala 22. marca 2021 závery[6] o stratégii kybernetickej bezpečnosti EÚ pre digitálnu dekádu, v ktorých vzala na vedomie nový návrh, ktorý vychádza zo smernice NIS, a opätovne potvrdila svoju podporu posilneniu a harmonizácii vnútroštátnych rámcov kybernetickej bezpečnosti a trvalej spolupráci medzi členskými štátmi.

8. Európska rada vyzvala v záveroch z 21. – 22. októbra 2021 k tomu, aby sa pokročilo v práci na návrhu revidovanej smernice NIS.

---

3 14133/20.
4 5573/21.
5 Stanovisko 5/2021 k stratégii kybernetickej bezpečnosti a smernici NIS 2.0.
6 6722/21.

II. PRÁCA V PRÍPRAVNÝCH ORGÁNOCH RADY

9. V Rade návrh skúma horizontálna pracovná skupina pre kybernetické otázky (ďalej len („HWPCI“). Preskúmanie návrhu sa začalo 19. januára počas portugalského predsedníctva, pričom návrh sa dôkladne prečítal, čo umožnilo členským štátom predložiť svoje otázky a zdôrazniť svoje hlavné obavy a dostať od Komisie podrobné vysvetlenia k zmenám v revidovanej smernici.

10. Počas portugalského predsedníctva sa venovalo prezentácii a čítaniu návrhu 17 zasadnutí HWPCI. Správa o pokroku týkajúca sa čítania bola predložená Rade TTE 4. júna 2021.

11. Práca potom pokračovala a zintenzívnila sa počas slovinského predsedníctva s cieľom dosiahnuť všeobecné smerovanie na zasadnutí Rady (doprava, telekomunikácie a energetika) 3. decembra 2021. Slovinské predsedníctvo venovalo 15 zasadnutí revízii návrhu NIS 2 a zorganizovalo mnohé dvojstranné rokovania na všetkých úrovniach.

12. HWPCI zamerala svoju prácu na prepracovanie znenia návrhu, pričom najprv sa sústredila na interakciu smernice NIS 2 s odvetvovými právnymi predpismi a rozsahom pôsobnosti, najmä pokiaľ ide o verejnú správu, koreňové servery DNS a doložku o vylúčení, a následne medzi iným na partnerské preskúmania, právomoc a vzájomnú pomoc, koordinované zverejňovanie informácií o zraniteľnosti, databázy doménových mien a registračných údajov a medzinárodnú spoluprácu.

13. Prvý kompromisný návrh týkajúci sa znenia navrhovanej smernice bol vydaný 21. septembra 2021[7], pričom vychádzal z písomných pripomienok a neoficiálnych dokumentov doručených členskými štátmi, ako aj zo skorších kompromisných návrhov o interakcii medzi smernicou NIS 2 a odvetvovými právnymi predpismi a o rozsahu pôsobnosti smernice NIS 2.

[7] 12019/21.

14. O najnovšej revízii[8] kompromisného návrhu predsedníctva sa rokovalo na úrovni pracovnej skupiny 22. novembra 2021. Hoci delegácie vo všeobecnosti kompromisné znenie uvítali, niektoré z nich vzniesli výhrady preskúmania alebo pripomienky k častiam kompromisného návrhu. K niektorým častiam znenia sa ešte navrhli zmeny technického typu.

III. NORMATÍVNE USTANOVENIA

15. Na základe rokovaní na úrovni pracovnej skupiny sa za hlavné politické otázky určili tieto oblasti:

a) Rozsah pôsobnosti (článok 2)

Od začiatku rokovaní o návrhu NIS 2 bol hlavnou obavou, ktorú vyjadrili členské štáty, výrazný nárast počtu subjektov, na ktoré sa smernica vzťahuje, a najmä zavedenie pravidla obmedzenia veľkosti, podľa ktorého všetky stredné a veľké subjekty, ktoré pôsobia v rámci príslušných odvetví alebo poskytujú služby, na ktoré sa vzťahuje smernica NIS 2, patria do rozsahu jej pôsobnosti. Hoci sa v kompromisnom návrhu toto všeobecné pravidlo zachováva, obsahuje aj dodatočné ustanovenia na zabezpečenie potrebnej proporcionality, vyššej úrovne riadenia rizika a jasných kritérií kritickosti na určenie subjektov, ktoré patria do rozsahu pôsobnosti smernice. Kompromisný návrh okrem toho obsahuje osobitné ustanovenia o uprednostňovaní využívania opatrení dohľadu, pri ktorom sa uplatňuje prístup založený na riziku.

[8] 12019/5/21 REV 5.

b) Verejná správa (článok 2 ods. 2a)

Zahrnutie verejnej správy do rozsahu pôsobnosti smernice NIS 2 bolo veľmi diskutovanou témou vzhľadom na to, že sektor verejnej správy je odlišnejší než ostatné sektory, na ktoré sa vzťahuje smernica NIS 2. Predsedníctvo sa usilovalo o vyvážený prístup, v ktorom sa zohľadnia osobitosti vnútroštátnych rámcov verejnej správy a zabezpečí sa, aby členské štáty mali určitý stupeň flexibility, pokiaľ ide o určenie subjektov verejnej správy, ktoré patria do rozsahu pôsobnosti NIS 2. V kompromisnom znení sa preto NIS 2 vzťahuje na subjekty verejnej správy ústredných vlád, zatiaľ čo členské štáty môžu stanoviť, že smernica sa vzťahuje aj na subjekty verejnej správy na regionálnej a miestnej úrovni.

c) Doložka o vylúčení (článok 2 ods. 3a a 3aa)

Členské štáty chceli ďalej objasniť doložku o vylúčení v tom zmysle, že smernica sa nevzťahuje na subjekty, ktoré vykonávajú primárne činnosti v oblasti obrany, národnej bezpečnosti, verejnej bezpečnosti alebo presadzovania práva, ani na činnosti týkajúce sa národnej bezpečnosti alebo obrany. Vylúčené sú aj súdy, parlamenty a centrálne banky.

d) Interakcia s odvetvovými právnymi predpismi

Členské štáty zdôraznili, že je potrebné zosúladiť smernicu NIS 2 s odvetvovými právnymi predpismi, najmä s nariadením o digitálnej prevádzkovej odolnosti finančného sektora (DORA) a so smernicou o odolnosti kritických subjektov (smernica CER). Smernica NIS 2, ktorá by mala predstavovať základ pre minimálnu harmonizáciu kybernetickej bezpečnosti, obsahuje osobitný článok o aktoch Únie platných pre jednotlivé odvetvia (článok 2b). Pokiaľ ide o interakciu so smernicou CER, kompromisný návrh lepšie objasňuje prístup „všetkých nebezpečenstiev“. Ďalšie dôležité doplnenia sa týkajú dohôd o spolupráci medzi príslušnými orgánmi podľa príslušných právnych aktov.

e) Partnerské zisťovanie (článok 16)

Až na niekoľko výnimiek boli členské štáty proti tomu, aby Komisia zaviedla povinné partnerské zisťovania. Navrhovaným kompromisom sa zabezpečuje, že nový mechanizmus partnerského zisťovania vychádza zo vzájomnej dôvery a je dobrovoľným procesom motivovaným členskými štátmi.

f) Právomoc a teritorialita (článok 24) a vzájomná pomoc (článok 34)

Členské štáty vyjadrili obavy v súvislosti s dôsledkami diferencovanej právomoci pre subjekty v odvetví IKT, ako navrhuje Komisia. V kompromisnom znení sa objasnila právomoc založená na druhu subjektov a tiež sa zdôraznili tie časti, ktoré sa týkajú vzájomnej pomoci.

g) Oznamovacie povinnosti (čl. 20)

Vzhľadom na obavy členských štátov, že oznamovacie povinnosti by nadmerne zaťažili subjekty, na ktoré sa vzťahuje smernica NIS 2, a viedli by k nadmernému podávaniu správ, sa v kompromisnom znení vylúčilo povinné nahlasovanie závažných kybernetických hrozieb.

IV. ZÁVER

16. Výbor stálych predstaviteľov dosiahol 24. novembra 2021 dohodu o kompromisnom znení uvedenom v prílohe a rozhodol o jeho predložení Rade (doprava, telekomunikácie a energetika) v záujme prijatia všeobecného smerovania.

17. Rada sa preto vyzýva, aby na zasadnutí 3. decembra 2021 schválila kompromisné znenie predložené predsedníctvom, ako sa uvádza v prílohe, a prijala všeobecné smerovanie.

PRÍLOHA

Návrh

SMERNICA EURÓPSKEHO PARLAMENTU A RADY

o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148

(Text s významom pre EHP)

EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE,

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

so zreteľom na návrh Európskej komisie,

po postúpení návrhu legislatívneho aktu národným parlamentom,

so zreteľom na stanovisko Európskeho hospodárskeho a sociálneho výboru[9],

so zreteľom na stanovisko Výboru regiónov[10],

konajúc v súlade s riadnym legislatívnym postupom,

[9] Ú. v. EÚ C , , s. .
[10] Ú. v. EÚ C , , s. .

keďže:

(1) Cieľom smernice Európskeho parlamentu a Rady (EÚ) 2016/1148[11] bolo budovať kybernetickobezpečnostné kapacity 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 kybernetickobezpečnostných incidentov, a tým prispievať k efektívnemu fungovaniu spoločnosti a hospodárstva Únie.

(2) Od nadobudnutia účinnosti smernice (EÚ) 2016/1148 sa pri zvyšovaní úrovne odolnosti Únie v oblasti kybernetickej bezpečnosti dosiahol významný pokrok. 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 vymedzením národných [...] stratégií v **oblasti bezpečnosti sietí a informačných systémov**, stanovením vnútroštátnych kapacít a vykonávaním regulačných opatrení vzťahujúcich sa na kľúčové infraštruktúry a aktérov identifikovaných v každom členskom štáte. Prispela aj k spolupráci na úrovni Únie zriadením skupiny pre spoluprácu[12] a siete [...] národných jednotiek pre riešenie počítačových bezpečnostných incidentov (ďalej len „sieť jednotiek CSIRT“)[13]. 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.

---

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

12 Článok 11 smernice (EÚ) 2016/1148.

13 Článok 12 smernice (EÚ) 2016/1148.

(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. Tento vývoj viedol k nárastu kybernetickobezpečnostných hrozieb a prináša nové výzvy, ktoré si vyžadujú prispôsobené, koordinované a inovatívne reakcie vo všetkých členských štátoch. Počet, rozsah, sofistikovanosť, frekvencia a vplyv kybernetickobezpečnostných incidentov sa zvyšujú a pre fungovanie sietí a informačných systémov predstavujú veľkú hrozbu. Vo výsledku môžu takéto 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 preto teraz pre riadne fungovanie vnútorného trhu dôležitejšie ako kedykoľvek predtým.

(4) Právnym základom smernice (EÚ) 1148/2016 bol článok 114 Zmluvy o fungovaní Európskej únie (ZFEÚ), ktorého cieľom je vytvorenie a fungovanie vnútorného trhu posilnením opatrení na aproximáciu vnútroštátnych pravidiel. Požiadavky na kybernetickú bezpečnosť uložené subjektom poskytujúcim služby alebo ekonomicky relevantné činnosti sa v jednotlivých členských štátoch značne líšia, pokiaľ ide o typ požiadaviek, ich úroveň podrobnosti a metódu dohľadu. Tieto rozdiely spôsobujú dodatočné náklady a podnikom, ktoré cezhranične ponúkajú tovar alebo služby, spôsobujú ťažkosti. Požiadavky jedného členského štátu, ktoré sa líšia od požiadaviek iného členského štátu alebo sú s nimi dokonca v rozpore, môžu tieto cezhraničné činnosti podstatne ovplyvniť.

Okrem toho môžu mať suboptimálne navrhnuté alebo zavedené kybernetickobezpečnostné [...] **opatrenia** v jednom členskom štáte vplyv na úroveň kybernetickej bezpečnosti v iných členských štátoch, najmä vzhľadom na intenzívne cezhraničné výmeny. Preskúmanie smernice (EÚ) 2016/1148 ukázalo, že pri jej implementácii členskými štátmi existujú veľké rozdiely, a to aj pokiaľ ide o jej rozsah pôsobnosti, ktorého určenie bolo do 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 implementáciu povinností týkajúcich sa bezpečnosti a oznamovania incidentov, ktoré sú v nej stanovené. Tieto povinnosti boli preto na vnútroštátnej úrovni implementované značne odlišne. Podobné rozdiely v implementácii sa vyskytli aj v súvislosti s ustanoveniami uvedenej smernice o dohľade a presadzovaní práva.

(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 kybernetickobezpečnostnej odolnosti v dôsledku uplatňovania rôznych [...] **opatrení.** 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 sankcií, ktoré sú nevyhnutné na účinné presadzovanie týchto povinností. Smernica (EÚ) 2016/1148 by sa preto mala zrušiť a nahradiť touto smernicou.

(6) [...] Členské štáty **by mali mať možnosť** prijať potrebné opatrenia s cieľom zaručiť ochranu základných záujmov vlastnej bezpečnosti, chrániť verejný poriadok a verejnú bezpečnosť a umožniť vyšetrovanie a odhaľovanie trestných činov, ako aj stíhanie ich páchateľov [...]. **Táto smernica by sa nemala vzťahovať na niektoré verejné alebo súkromné subjekty, ktoré vykonávajú činnosti v týchto oblastiach. Rovnako by sa nemala vzťahovať na činnosti subjektov vykonávané v týchto oblastiach. Navyše** v súlade s článkom 346 ZFEÚ nemá byť žiaden členský štát povinný poskytovať informácie, ktorých sprístupnenie by odporovalo základným záujmom jeho verejnej bezpečnosti. [...] Relevantné sú pravidlá členských štátov [...] **alebo** Únie na ochranu utajovaných skutočností, dohody o zachovaní mlčanlivosti a neformálne dohody o zachovaní mlčanlivosti, ako napríklad semaforový protokol[14].

(6a) Na každé spracúvanie osobných údajov podľa tejto smernice sa vzťahuje právo Únie týkajúce sa ochrany osobných údajov a súkromia. Predovšetkým, touto smernicou nie je dotknuté nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 a smernica Európskeho parlamentu a Rady 2002/58/ES, a preto by táto smernica nemala mať vplyv najmä na úlohy a právomoci nezávislých dozorných orgánov príslušných na monitorovanie dodržiavania príslušného práva Únie týkajúceho sa ochrany údajov.

---

14 Semaforový protokol (Traffic Light Protocol, TLP) slúži pri sprístupňovaní informácií na informovanie príjemcov o akýchkoľvek obmedzeniach pri ďalšom šírení týchto informácií. Používa sa takmer vo všetkých komunitách jednotiek CSIRT a v niektorých strediskách pre výmenu a analýzu informácií (ISAC).

(7) Zrušením smernice (EÚ) 2016/1148 by sa rozsah uplatňovania podľa odvetví mal rozšíriť na väčšiu časť hospodárstva vzhľadom na úvahy uvedené v odôvodneniach 4 až 6. Odvetvia, na ktoré sa vzťahuje smernica (EÚ) 2016/1148, by sa preto mali rozšíriť tak, aby boli komplexne pokryté odvetvia a služby, ktoré majú zásadný význam pre kľúčové spoločenské a hospodárske činnosti v rámci vnútorného trhu. Pravidlá by sa nemali líšiť podľa toho, či sú subjekty prevádzkovateľmi základných služieb alebo poskytovateľmi digitálnych služieb. Takéto rozlišovanie sa ukázalo ako zastarané, pretože neodráža skutočný význam odvetví alebo služieb pre spoločenské a hospodárske činnosti na vnútornom trhu.

(8) V súlade so smernicou (EÚ) 2016/1148 boli členské štáty zodpovedné za určenie tých subjektov, ktoré spĺňajú kritériá, aby mohli pôsobiť ako prevádzkovatelia základných služieb („proces identifikácie“). S cieľom odstrániť v tejto súvislosti veľké rozdiely medzi členskými štátmi a zabezpečiť právnu istotu, pokiaľ ide o požiadavky na riadenie 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. Toto kritérium by malo spočívať v uplatňovaní pravidla obmedzenia veľkosti, podľa ktorého všetky stredné a veľké podniky, ako sú vymedzené v odporúčaní Komisie 2003/361/ES[15], ktoré pôsobia v rámci takých odvetví alebo poskytujú taký druh služieb, na ktoré sa vzťahuje táto smernica, patria do rozsahu jej pôsobnosti. [...]

[15] Odporúčanie Komisie 2003/361/ES zo 6. mája 2003 o vymedzení pojmov mikro, malé a stredné podniky (Ú. v. EÚ L 124, 20.5.2003, s. 36).

(8a) S cieľom zabezpečiť jasný prehľad o subjektoch, ktoré patria do rozsahu pôsobnosti tejto smernice, by členské štáty mali mať možnosť zaviesť vnútroštátne mechanizmy na oznamovanie vlastných údajov, ktorými sa od subjektov, na ktoré sa vzťahuje táto smernica, vyžaduje, aby príslušným orgánom podľa tejto smernice alebo orgánom, ktoré na tento účel určili členské štáty, predložili aspoň svoj názov, adresu a kontaktné údaje, ako aj odvetvie, v ktorom pôsobia, alebo druh služby, ktorú poskytujú, a prípadne zoznam členských štátov, v ktorých daný subjekt poskytuje svoje služby. Členské štáty môžu rozhodnúť o vhodných mechanizmoch, ak na vnútroštátnej úrovni existujú registre, ktoré umožňujú identifikáciu subjektov, ktoré patria do rozsahu pôsobnosti tejto smernice.

(9) Táto smernica by sa [...] mala vzťahovať aj na **mikrosubjekty alebo** malé subjekty [...] spĺňajúce určité kritériá, ktoré sú ukazovateľom kľúčovej úlohy pre hospodárstva alebo spoločnosti členských štátov alebo pre určité odvetvia či druhy služieb. Členské štáty by mali byť zodpovedné za [...] to, že Komisii predložia [...] **aspoň relevantné informácie o počte identifikovaných subjektov, o odvetví, do ktorého patria, alebo o druhu služby, ktorú poskytujú, a o osobitných kritériách, na základe ktorých boli identifikované. Členské štáty sa tiež môžu rozhodnúť, že Komisii predložia názvy týchto subjektov, ak je to v súlade s vnútroštátnymi bezpečnostnými predpismi.**

(9a) Subjekty verejnej správy, ktoré vykonávajú činnosti v oblasti národnej bezpečnosti, obrany, verejnej bezpečnosti, presadzovania práva, ako aj súdnictva, parlamenty a centrálne banky, sú 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 týchto dôvodov vylúčené z rozsahu pôsobnosti tejto smernice. Do rozsahu pôsobnosti tejto smernice nepatria ani subjekty verejnej správy na úrovni ústrednej štátnej správy, ktoré sú zriadené spoločne s treťou krajinou v súlade s medzinárodnou dohodou.

(9aa) Členské štáty by mali mať možnosť stanoviť, aby sa subjekty, ktoré boli pred nadobudnutím účinnosti tejto smernice označené za prevádzkovateľov základných služieb v súlade so smernicou (EÚ) 2016/1148, považovali za kľúčové subjekty.

(9aaa) Táto smernica sa nevzťahuje na diplomatické a konzulárne misie členských štátov v zahraničí a na ich infraštruktúru IKT, ktorú takéto misie využívajú, pokiaľ je takáto infraštruktúra umiestnená v zahraničí alebo sa prevádzkuje pre používateľov v zahraničí.

(10) Komisia môže v spolupráci so skupinou pre spoluprácu vydať usmernenia o vykonávaní kritérií uplatniteľných na mikropodniky a malé podniky.

(11) **[...] Subjekty, ktoré patria do rozsahu pôsobnosti tejto smernice, by sa mali rozdeliť do dvoch kategórií: kľúčové a dôležité, pričom by sa mala zohľadňovať úroveň kritickosti daného odvetvia alebo druhu služieb, ktoré poskytujú, ako aj ich veľkosť. V tejto súvislosti by sa v relevantných prípadoch mali náležite zohľadniť aj všetky relevantné odvetvové posúdenia rizík alebo usmernenia zo strany príslušných orgánov. Na** kľúčové aj dôležité subjekty by sa mali vzťahovať [...] požiadavky na riadenie rizík a oznamovacie povinnosti. Malo by sa rozlišovať medzi režimom dohľadu a sankcií, pokiaľ ide o 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.

(12) **V tejto smernici sa stanovuje základ pre opatrenia na riadenie kybernetickobezpečnostných rizík a pre oznamovacie povinnosti vo všetkých odvetviach, ktoré patria do jej rozsahu pôsobnosti. Aby sa zabránilo fragmentácii ustanovení o kybernetickej bezpečnosti v rámci právnych aktov Únie, by v prípade, ak sa v záujme zabezpečenia vysokej úrovne kybernetickej bezpečnosti považujú za potrebné dodatočné ustanovenia platné pre jednotlivé odvetvia, ktoré sa týkajú** opatrení na riadenie kybernetickobezpečnostných rizík a **oznamovacích povinností, mala Komisia posúdiť, či by sa takéto ustanovenia mohli ustanoviť vo vykonávacom akte na základe splnomocnenia udeleného v tejto smernici.** V prípade, a**k by takéto akty neboli na tento účel vhodné,** k zabezpečeniu vysokej úrovne [...] kybernetickej bezpečnosti **by mohli** prispieť právne predpisy platné pre jednotlivé odvetvia, pričom by sa v nich plne zohľadnili špecifiká a zložitosti [...] **dotknutých** odvetví. **V právnych predpisoch platných pre jednotlivé odvetvia je potrebné zdôvodniť, prečo nebol vykonávací akt na základe splnomocnenia udeleného v tejto smernici vhodný. Takéto ustanovenia právnych aktov Únie platných pre jednotlivé odvetvia by zároveň mali náležite zohľadňovať potrebu komplexného a harmonizovaného rámca kybernetickej bezpečnosti.** [...] Týmto [...] nie sú dotknuté existujúce vykonávacie právomoci, ktoré boli na [...] Komisiu prenesené vo viacerých odvetviach vrátane dopravy a energetiky.

(12a) Ak právny akt Únie platný pre jednotlivé odvetvia **obsahuje ustanovenia**, [...] v ktorých sa vyžaduje, aby kľúčové alebo dôležité subjekty prijali **opatrenia, ktoré majú aspoň rovnocenný účinok ako povinnosti stanovené v tejto smernici týkajúce sa** riadenia kybernetickobezpečnostných rizík [...] a **povinností** oznamovať **významné** incidenty alebo významné kybernetické hrozby [...], mali by sa uplatňovať dané ustanovenia platné pre jednotlivé odvetvia **vrátane ustanovení o dohľade a presadzovaní práva**. **Pri určovaní rovnocenného účinku povinností stanovených v ustanoveniach právneho aktu Únie platného pre jednotlivé odvetvia by sa mali zvážiť tieto aspekty: i) opatrenia na riadenie kybernetickobezpečnostných rizík by mali pozostávať z náležitých a primeraných technických a organizačných opatrení na riadenie rizík súvisiacich s bezpečnosťou sietí a informačných systémov, ktoré relevantné subjekty používajú pri poskytovaní svojich služieb, a mali by zahŕňať minimálne všetky prvky stanovené v tejto smernici; ii) povinnosť oznamovať významné incidenty a kybernetické hrozby by mala byť aspoň rovnocenná s povinnosťami stanovenými v tejto smernici, pokiaľ ide o obsah, formát a lehoty oznámení; iii) modality oznamovania právnych aktov Únie platných pre jednotlivé odvetvia zo strany subjektov a príslušných orgánov by mali byť aspoň rovnocenné s požiadavkami stanovenými v tejto smernici, pokiaľ ide o ich obsah, formát a lehoty, a mali by zohľadňovať úlohu jednotiek CSIRT; iv) požiadavky na cezhraničnú spoluprácu, ktoré sa týkajú relevantných orgánov, by mali byť aspoň rovnocenné s požiadavkami stanovenými v tejto smernici. Ak sa ustanovenia právneho aktu Únie platného pre jednotlivé odvetvia nevzťahujú na všetky subjekty v konkrétnom odvetví, ktoré patria do rozsahu pôsobnosti tejto smernice, na subjekty, na ktoré sa nevzťahujú dané ustanovenia platné pre jednotlivé odvetvia, by sa mali naďalej uplatňovať príslušné ustanovenia tejto smernice.**

(12aa) Komisia **by mala pravidelne preskúmavať uplatňovanie požiadavky na rovnocenný účinok vo vzťahu k ustanoveniam právnych aktov Únie platných pre jednotlivé odvetvia** [...]. **Komisia má pri príprave tohto pravidelného preskúmania konzultovať so skupinou pre spoluprácu.**

(12aaa) Budúce právne akty Únie platné pre jednotlivé odvetvia by mali náležite zohľadňovať vymedzenia pojmov uvedené v článku 4 tejto smernice a rámec dohľadu a presadzovania práva stanovený v kapitole VI tejto smernice.

(12ab) Ak sa v ustanoveniach právnych aktov Únie platných pre jednotlivé odvetvia vyžaduje, aby kľúčové alebo dôležité subjekty prijali opatrenia, ktoré majú aspoň rovnocenný účinok ako oznamovacie povinnosti stanovené v tejto smernici, malo by sa zabrániť prekrývaniu oznamovacích povinností a mala by sa zabezpečiť koherentnosť a účinnosť vybavovania oznámení o kybernetických hrozbách alebo incidentoch. Na tento účel môžu tieto ustanovenia platné pre jednotlivé odvetvia umožniť členským štátom vytvoriť spoločný, automatický a priamy mechanizmus oznamovania významných incidentov a kybernetických hrozieb orgánom, ktorých úlohy sú stanovené v príslušných ustanoveniach platných pre jednotlivé odvetvia, ako aj príslušným orgánom vrátane jednotného kontaktného miesta a jednotiek CSIRT, ak je to vhodné, ktoré sú zodpovedné za úlohy v oblasti kybernetickej bezpečnosti stanovené v tejto smernici, alebo mechanizmus, ktorým sa zabezpečuje systematické a okamžité zdieľanie informácií a spolupráca medzi relevantnými orgánmi a jednotkami CSIRT pri vybavovaní takýchto oznámení. Na účely zjednodušenia oznamovania a vykonávania spoločného, automatického a priameho mechanizmu oznamovania môžu členské štáty v súlade s právnymi predpismi platnými pre jednotlivé odvetvia využívať jednotný vstupný bod, ktorý zriadia podľa článku 11 ods. 5a tejto smernice. S cieľom zabezpečiť harmonizáciu by sa oznamovacie povinnosti vyplývajúce z právnych aktov Únie platných pre jednotlivé odvetvia mali zosúladiť s povinnosťami stanovenými v tejto smernici. Členské štáty môžu určiť, aby príslušné orgány podľa tejto smernice alebo vnútroštátne jednotky CSIRT boli adresátmi oznamovania v súlade s právnymi predpismi platnými pre jednotlivé odvetvia.

(13) Nariadenie Európskeho parlamentu a Rady XXXX/XXXX by sa v súvislosti s touto smernicou malo považovať za právny akt Únie platný pre jednotlivé odvetvie, pokiaľ ide o subjekty finančného odvetvia. Namiesto ustanovení **stanovených** [...] v tejto smernici by sa mali uplatňovať ustanovenia nariadenia XXXX/XXXX týkajúce sa opatrení na riadenie rizík v oblasti informačných a komunikačných technológií (IKT), riadenia incidentov súvisiacich s IKT, a najmä oznamovania incidentov, ako aj testovania digitálnej prevádzkovej odolnosti, mechanizmov zdieľania informácií a rizík týkajúcich sa IKT zabezpečovaných tretími stranami. Členské štáty by preto nemali uplatňovať ustanovenia tejto smernice týkajúce sa riadenia kybernetickobezpečnostných rizík [...] a oznamovacích povinností, a tiež dohľadu a presadzovania práva na [...] finančné subjekty, na ktoré sa vzťahuje nariadenie XXXX/XXXX. Zároveň je dôležité zachovať pevné vzťahy a výmenu informácií s finančným odvetvím podľa tejto smernice. Na tento účel nariadenie XXXX/XXXX umožňuje [...] európskym orgánom dohľadu (ESA) vo finančnom odvetví a príslušným vnútroštátnym orgánom podľa nariadenia XXXX/XXXX [...] zúčastňovať sa na [...] **práci** [...] skupiny pre spoluprácu a vymieňať si informácie a spolupracovať s jednotnými kontaktnými miestami určenými podľa tejto smernice, [...] **ako aj** s vnútroštátnymi jednotkami CSIRT. Príslušné orgány podľa nariadenia XXXX/XXXX by mali zasielať podrobnosti o závažných incidentoch súvisiacich s IKT a **významných kybernetických hrozbách** aj jednotným kontaktným miestam, **príslušným orgánom alebo vnútroštátnym jednotkám CSIRT** určeným podľa tejto smernice. **To možno dosiahnuť automatickým a priamym postupovaním oznámení o incidentoch alebo prostredníctvom spoločnej platformy na oznamovanie.** Členské štáty by okrem toho mali naďalej začleňovať finančné odvetvie do svojich stratégií kybernetickej bezpečnosti a vnútroštátne jednotky CSIRT môžu zahrnúť finančné odvetvie do svojich činností.

(13a) Aby sa zabránilo medzerám a duplicite, pokiaľ ide o povinnosti v oblasti kybernetickej bezpečnosti uložené subjektom v odvetví letectva uvedeným v bode 2 písm. a) prílohy I, by vnútroštátne orgány určené podľa nariadení Európskeho parlamentu a Rady (ES) č. 300/2008[16] a (EÚ) 2018/1139[17] a príslušné orgány podľa tejto smernice mali spolupracovať v súvislosti s vykonávaním opatrení na riadenie kybernetickobezpečnostných rizík a dohľadom nad týmito opatreniami na vnútroštátnej úrovni. Dodržiavanie opatrení na riadenie kybernetickobezpečnostných rizík podľa tejto smernice [...] zo strany subjektu by vnútroštátne orgány určené podľa nariadení (ES) č. 300/2008 a (EÚ) 2018/1139 mohli považovať za spĺňanie požiadaviek stanovených v uvedených nariadeniach a v príslušných delegovaných a vykonávacích aktoch prijatých podľa uvedených nariadení.

---

16 **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).**

17 **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 mení nariadenia Európskeho parlamentu a Rady (ES) č. 2111/2005, (ES) č. 1008/2008, (EÚ) č. 996/2010, (EÚ) č. 376/2014 a smernice Európskeho parlamentu a Rady 2014/30/EÚ a 2014/53/EÚ a zrušujú nariadenia Európskeho parlamentu a Rady (ES) č. 552/2004 a (ES) č. 216/2008 a nariadenie Rady (EHS) č. 3922/91 (Ú. v. EÚ L 212, 22.8.2018, s. 1).**

(14) Vzhľadom na prepojenia medzi kybernetickou bezpečnosťou a fyzickou bezpečnosťou subjektov by sa mal zabezpečiť jednotný prístup medzi smernicou Európskeho parlamentu a Rady (EÚ) XXX/XXX a touto smernicou. Na dosiahnutie tohto cieľa by členské štáty mali zabezpečiť, aby sa kritické subjekty **[**a rovnocenné subjekty**]** podľa smernice (EÚ) XXX/XXX považovali za kľúčové subjekty podľa tejto smernice. Členské štáty by tiež mali zabezpečiť, aby ich stratégie kybernetickej bezpečnosti poskytovali politický rámec pre posilnenú koordináciu medzi príslušným orgánom podľa tejto smernice a príslušným orgánom podľa smernice (EÚ) XXX/XXX v kontexte zdieľania informácií o incidentoch a kybernetických hrozbách, ako aj vykonávania úloh dohľadu. **Príslušné** [...] orgány podľa oboch smerníc by mali spolupracovať a vymieňať si informácie, najmä pokiaľ ide o identifikáciu kritických subjektov, kybernetické hrozby, kybernetickobezpečnostné riziká, incidenty, **ako aj nekybernetické riziká, hrozby a incidenty**, ktoré ovplyvňujú kritické subjekty **[**alebo **subjekty rovnocenné s kritickými subjektmi],** [...] **vrátane** kybernetickobezpečnostných a **fyzických** opatrení prijatých kritickými subjektmi a **výsledkov činností dohľadu vykonávaných v súvislosti s týmito subjektmi. Okrem toho s cieľom zefektívniť činnosti dohľadu medzi príslušnými orgánmi určenými podľa oboch smerníc a s cieľom minimalizovať administratívnu záťaž dotknutých subjektov by sa príslušné orgány mali usilovať zharmonizovať vzorové formuláre na oznamovanie incidentov a postupy dohľadu.** [...] **V náležitých prípadoch môžu** príslušné orgány podľa smernice (EÚ) XXX/XXX [...] **požiadať** príslušné orgány podľa tejto smernice [...], aby vykonávali svoje právomoci v oblasti dohľadu a presadzovania práva [...] vo **vzťahu ku** kľúčovému subjektu identifikovanému ako kritický subjekt.[...] [...]

(14a) Subjekty patriace do odvetvia digitálnej infraštruktúry sú v podstate založené na sieťach a informačných systémoch, a preto by sa povinnosti, ktoré týmto subjektom ukladá táto smernica, mali komplexným spôsobom zaoberať fyzickou bezpečnosťou takýchto systémov ako súčasť ich povinností v oblasti riadenia kybernetickobezpečnostných rizík a oznamovacích povinností. Keďže sa na uvedené záležitosti vzťahuje táto smernica, povinnosti stanovené v kapitolách III až VI smernice (EÚ) XXX/XXX [CER] sa na takéto subjekty nevzťahujú.

(15) Potvrdenie a udržanie spoľahlivého, odolného a bezpečného systému doménových mien (DNS) je kľúčovým faktorom zachovania integrity internetu a je nevyhnutné pre jeho nepretržité a stabilné fungovanie, od ktorého závisí digitálne hospodárstvo a spoločnosť. Táto smernica by sa preto mala vzťahovať na poskytovateľov služieb DNS v reťazci **poskytovania a** riešenia DNS, **ktoré majú význam pre vnútorný trh**, vrátane [...] **správcov mien** [...] domén najvyššej úrovne (TLD), **subjektov poskytujúcich služby registrácie mien domén, prevádzkovateľov** autoritatívnych menných serverov pre doménové mená a **prevádzkovateľov** rekurzívnych resolverov. **Pojem „poskytovateľ služieb DNS“ by sa nemal vzťahovať na služby DNS prevádzkované na vlastné účely dotknutého subjektu a jeho pridružených subjektov. Povinnosti v oblasti kybernetickej bezpečnosti vyplývajúce z tejto smernice pre túto kategóriu poskytovateľov sú prísne obmedzené na opatrenia na riadenie kybernetickobezpečnostných rizík a oznamovanie, a preto nimi nie je dotknutá správa globálnych DNS komunitou viacerých zainteresovaných strán.**

(16) Služby cloud computingu by sa mali vzťahovať na služby, ktoré umožňujú správu na požiadanie a vzdialený širokopásmový prístup ku škálovateľnému a pružnému súboru zdieľateľných a distribuovaných počítačových zdrojov. Uvedené počítačové zdroje zahŕňajú zdroje, ako sú napríklad 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. Uvedené modely služieb a zavádzania majú rovnaký význam ako podmienky poskytovania služieb a modely zavádzania 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, 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 tých 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 tých 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 tých počítačových zdrojov, ktoré sa nachádzajú v rôznych sieťových počítačoch alebo zariadeniach a ktoré navzájom komunikujú a koordinujú sa prenosom správ.

(17) Vzhľadom na vznik inovačných technológií a nových obchodných modelov sa očakáva, že sa na trhu objavia nové modely zavádzania cloud computingu a služieb 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“).

(18) 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 zvládnuť všetky riziká spojené s bezpečnosťou sietí a informačných systémov by sa táto smernica mala vzťahovať aj na poskytovateľov takých 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 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“ sa nevzťahuje na interné, podnikové dátové centrá vlastnené a prevádzkované na vlastné účely príslušného subjektu.

(19) Poskytovatelia poštových služieb v zmysle smernice Európskeho parlamentu a Rady 97/67/ES[18] [...] **vrátane** poskytovateľov [...] kuriérskych [...] služieb by mali podliehať tejto smernici, ak zabezpečujú aspoň jeden z krokov v reťazci poštového doručovania, a to najmä vyberanie, triedenie alebo distribúciu vrátane služieb zberu. Dopravné služby, ktoré sa nevykonávajú v spojení s jedným z týchto krokov, by nemali patriť do rozsahu poštových služieb.

---

18 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).

(20) Táto rastúca previazanosť je výsledkom čoraz väčšej cezhraničnej a previazanej siete poskytovania služieb s využitím kľúčových infraštruktúr v celej Únii v odvetviach energetiky, dopravy, digitálnej infraštruktúry, pitnej a odpadovej vody, zdravia, určitých aspektov verejnej správy, ako aj kozmického priestoru, pokiaľ ide o poskytovanie určitých služieb v závislosti od pozemných infraštruktúr, ktoré vlastnia, spravujú a prevádzkujú členské štáty alebo súkromné strany, a preto sa nevzťahujú na infraštruktúry vlastnené, spravované alebo prevádzkované Úniou alebo v jej mene ako súčasť jej vesmírnych programov. 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. Pandémia ochorenia COVID-19 ukázala zraniteľnosť našich čoraz previazanejších spoločností voči rizikám s nízkou pravdepodobnosťou.

(**20a**) **V záujme dosiahnutia a udržania vysokej úrovne kybernetickej bezpečnosti by národné stratégie kybernetickej bezpečnosti vyžadované touto smernicou mali pozostávať zo súdržných rámcov, ktoré zabezpečujú riadenie v oblasti kybernetickej bezpečnosti. Tieto stratégie môžu pozostávať z jedného alebo viacerých dokumentov legislatívnej alebo nelegislatívnej povahy.**

(21) Vzhľadom na rozdiely vo vnútroštátnych štruktúrach riadenia a s cieľom chrániť už existujúce odvetvové dohody alebo orgány dohľadu a regulačné orgány Únie by členské štáty mali mať možnosť určiť viac než jeden vnútroštátny príslušný orgán zodpovedný za vykonávanie úloh súvisiacich s bezpečnosťou sietí a informačných systémov kľúčových a dôležitých subjektov podľa tejto smernice. Členské štáty by mali mať možnosť poveriť touto úlohou existujúci orgán.

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

(23) Príslušné orgány alebo jednotky CSIRT by mali dostávať oznámenia o incidentoch od subjektov účinným a efektívnym spôsobom**, a to aj s cieľom uľahčiť v prípade potreby včasnú reakciu na incidenty a poskytnúť oznamujúcemu subjektu reakciu.** Malo by byť úlohou jednotných kontaktných miest postupovať oznámenia o incidentoch jednotným kontaktným miestam ostatných dotknutých členských štátov. [...]

(23a) V právnych aktoch Únie platných pre jednotlivé odvetvia, ktoré vyžadujú opatrenia na riadenie kybernetickobezpečnostných rizík alebo oznamovacie povinnosti, ktoré majú aspoň rovnocenný účinok ako tie, ktoré sú stanovené v tejto smernici, by sa mohlo stanoviť, že ich určené príslušné orgány vykonávajú svoje právomoci v oblasti dohľadu a presadzovania práva vo vzťahu k takýmto opatreniam alebo povinnostiam s pomocou príslušných orgánov určených v súlade s touto smernicou. Dotknuté príslušné orgány by na tento účel mohli uzavrieť dohody o spolupráci. V takýchto dohodách o spolupráci by sa okrem iného mohli špecifikovať postupy týkajúce sa koordinácie činností dohľadu vrátane postupov vyšetrovaní a kontrol na mieste v súlade s vnútroštátnym právom a mechanizmu výmeny relevantných informácií medzi príslušnými orgánmi, pokiaľ ide o dohľad a presadzovanie práva, vrátane prístupu k informáciám súvisiacim s kybernetikou, ktoré požadujú príslušné orgány určené v súlade s touto smernicou.

(24) Členské štáty by mali mať primerané vybavenie, pokiaľ ide o technické a organizačné kapacity, aby mohli predchádzať incidentom a rizikám v oblasti sietí a informačných systémov, odhaľovať ich, reagovať na ne a zmierňovať ich. Členské štáty by preto mali zabezpečiť, aby mali dobre fungujúce jednotky CSIRT, známe aj ako jednotky reakcie na núdzové počítačové situácie (ďalej len „jednotky CERT“), ktoré budú dodržiavať základné požiadavky s cieľom zaručiť účinné a zlučiteľné kapacity na riešenie incidentov a rizík a zabezpečiť účinnú spoluprácu na úrovni Únie. S cieľom posilniť dôverný vzťah medzi subjektmi a jednotkami CSIRT v prípadoch, keď je jednotka CSIRT súčasťou príslušného orgánu, **môžu** členské štáty [...] zvážiť funkčné oddelenie operačných úloh poskytovaných jednotkami CSIRT, najmä pokiaľ ide o zdieľanie informácií a podporu subjektov, od činností dohľadu príslušných orgánov.

(25) Pokiaľ ide o osobné údaje, jednotky CSIRT by mali mať možnosť vykonávať v súlade s nariadením Európskeho parlamentu a Rady (EÚ) 2016/679[19] v mene subjektu a na jeho žiadosť podľa tejto smernice proaktívnu kontrolu sietí a informačných systémov používaných na poskytovanie jeho služieb. **V prípade potreby** by sa členské štáty mali zamerať na zabezpečenie rovnakej úrovne technických kapacít pre všetky odvetvové jednotky CSIRT. Členské štáty môžu pri tvorbe vnútroštátnych jednotiek CSIRT požiadať o pomoc Agentúru Európskej únie pre kybernetickú bezpečnosť (ENISA).

(26) 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 si preto mohli vymieňať informácie vrátane osobných údajov s jednotkami CSIRT z tretích krajín alebo ich orgánmi na účely vykonávania svojich úloh v súlade s nariadením (EÚ) 2016/679. V prípadoch, keď neexistuje rozhodnutie o primeranosti prijaté v súlade s článkom 45 nariadenia (EÚ) 2016/679 alebo ak neexistujú primerané záruky podľa článku 46 uvedeného nariadenia, by sa výmena osobných údajov, ktorá sa považuje za nevyhnutnú na účely zmiernenia významných kybernetických hrozieb a na účely reakcie na prebiehajúci významný incident, mohla považovať za dôležitý dôvod verejného záujmu v zmysle článku 49 ods. 1 písm. d) nariadenia (EÚ) 2016/679.**

---

19 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).

(27) V súlade s prílohou k odporúčaniu Komisie (EÚ) 2017/1548 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu (ďalej len „koncepcia“)[20] by incident veľkého rozsahu mal znamenať incident s významným dosahom na najmenej dva členské štáty alebo ktorý svojím narušením presahuje schopnosť členského štátu reagovať naň. Incidenty veľkého rozsahu sa v závislosti od svojej príčiny a dosahu môžu vystupňovať a naplno prepuknúť v krízu, ktorá neumožňuje riadne fungovanie vnútorného trhu. Vzhľadom na široký rozsah a vo väčšine prípadov cezhraničný charakter takýchto incidentov by členské štáty a príslušné inštitúcie, orgány a agentúry Únie mali spolupracovať na technickej, prevádzkovej a politickej úrovni s cieľom riadne koordinovať reakciu v celej Únii.

(28) Keďže využívanie zraniteľností v sieťach a informačných systémoch môže spôsobiť značné narušenie a škody, rýchla identifikácia a náprava týchto zraniteľností je dôležitým faktorom pri znižovaní kybernetickobezpečnostného rizika. Subjekty, ktoré takéto systémy vyvíjajú **alebo spravujú**, by preto mali zaviesť vhodné postupy na riešenie zistených zraniteľností. Keďže zraniteľnosti často odhaľujú a oznamujú (zverejňujú) tretie strany (oznamujúce subjekty), výrobca alebo poskytovateľ produktov alebo služieb IKT by mal zaviesť aj potrebné postupy na získavanie informácií o zraniteľnosti od tretích strán. V tejto súvislosti sa v medzinárodnej norme ISO/IEC 30111 poskytujú usmernenia na riešenie zraniteľností a v medzinárodnej norme ISO/IEC [...] **29147** zasa usmernenia na zverejňovanie informácií o zraniteľnosti. Pokiaľ ide o zverejňovanie informácií o zraniteľnosti, obzvlášť dôležitá je koordinácia medzi oznamujúcimi subjektmi a výrobcami alebo poskytovateľmi produktov alebo služieb IKT. Koordinované zverejňovanie informácií o zraniteľnosti sa riadi štruktúrovaným procesom, v rámci ktorého sa zraniteľnosti hlásia organizáciám takým spôsobom, ktorým sa danej organizácii umožňuje diagnostikovať zraniteľnosť a zabezpečiť jej nápravu pred tým, ako sa podrobné informácie o zraniteľnosti poskytnú tretím stranám alebo verejnosti. Koordinované zverejňovanie informácií o zraniteľnosti by malo zahŕňať aj koordináciu medzi oznamujúcim subjektom a organizáciou, pokiaľ ide o načasovanie nápravy a zverejnenie zraniteľností.

---

[20] 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).

(29) Členské štáty by preto mali prijať opatrenia na uľahčenie koordinovaného zverejňovania informácií o zraniteľnostiach zavedením príslušnej vnútroštátnej politiky. **V rámci svojej vnútroštátnej politiky by sa členské štáty mali snažiť v čo najväčšej miere riešiť výzvy, ktorým čelia výskumníci zaoberajúci sa zraniteľnosťami, vrátane ich možného rizika trestnej zodpovednosti, v súlade so svojím vnútroštátnym právnym poriadkom.** [...] Členské štáty by mali určiť jednotku CSIRT, ktorá by prevzala úlohu „koordinátora“, ktorý by v prípade potreby pôsobil ako sprostredkovateľ medzi oznamujúcimi subjektmi a výrobcami alebo poskytovateľmi produktov alebo služieb IKT. Úlohy koordinátora jednotiek CSIRT by mali zahŕňať najmä identifikáciu a kontaktovanie dotknutých subjektov, podporu oznamujúcich subjektov, rokovania o harmonograme zverejňovania informácií a riadenie zraniteľností, ktoré majú vplyv na viaceré organizácie (viacstranné **koordinované** zverejňovanie informácií o zraniteľnosti). Ak **by oznámená zraniteľnosť mohla mať potenciálne významný vplyv na subjekty** [...] vo viac ako jednom členskom štáte, určené jednotky CSIRT [...] by mali v **prípade potreby** spolupracovať v rámci siete jednotiek CSIRT.

(30) Prístup k správnym a včasným informáciám o zraniteľnostiach ovplyvňujúcich produkty a služby IKT prispieva k lepšiemu riadeniu kybernetickobezpečnostných rizík. V tejto súvislosti sú zdroje verejne dostupných informácií o zraniteľnostiach dôležitým nástrojom pre subjekty a ich používateľov, ale aj pre príslušné vnútroštátne orgány a jednotky CSIRT. Agentúra ENISA by preto mala zriadiť register zraniteľností, v ktorom by kľúčové a dôležité subjekty a ich dodávatelia, ako aj subjekty, ktoré nepatria do rozsahu pôsobnosti tejto smernice, **alebo určené jednotky CSIRT** mohli dobrovoľne zverejňovať zraniteľnosti a poskytovať o nich informácie, ktoré používateľom umožnia prijať vhodné zmierňujúce opatrenia.

(31) Hoci podobné registre alebo databázy zraniteľností existujú, ich hostiteľmi a správcami sú subjekty, ktoré nie sú usadené v Únii. Európsky register zraniteľností, ktorý vedie agentúra ENISA, by zabezpečil lepšiu transparentnosť, pokiaľ ide o proces uverejňovania pred tým, ako je daná zraniteľnosť oficiálne oznámená, ako aj odolnosť v prípade narušenia alebo prerušenia poskytovania podobných služieb. Agentúra ENISA by mala preskúmať možnosť uzatvorenia dohôd o štruktúrovanej spolupráci s podobnými registrami v jurisdikciách tretích krajín s cieľom zabrániť duplicite úsilia a usilovať sa v čo najväčšej možnej miere o komplementaritu. **Agentúra ENISA by mala preskúmať najmä možnosť úzkej spolupráce s prevádzkovateľmi systému spoločných zraniteľností a expozícií (CVE – *Common Vulnerabilities and Exposures*) vrátane možnosti stať sa hlavným orgánom pre prideľovanie čísel CVE.**

(32) **Skupina pre spoluprácu by mala naďalej podporovať a uľahčovať strategickú spoluprácu a výmenu informácií, a tiež posilňovať dôveru medzi členskými štátmi.** Skupina pre spoluprácu by mala každé dva roky vypracovať pracovný program vrátane opatrení, ktoré má skupina vykonať na plnenie svojich cieľov a úloh. Časový rámec prvého programu prijatého podľa tejto smernice by sa mal zosúladiť s časovým rámcom posledného programu prijatého podľa smernice (EÚ) 2016/1148 s cieľom zabrániť možným narušeniam práce skupiny.

(33) 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, ktorými sa má dosiahnuť lepšie vykonávanie existujúcich pravidiel.

(34) 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. Mala by organizovať pravidelné spoločné stretnutia s príslušnými súkromnými zainteresovanými stranami z celej Únie s cieľom prediskutovať činnosti skupiny a zhromažďovať informácie o nových politických výzvach. S cieľom posilniť spoluprácu na úrovni Únie by skupina mala zvážiť prizývanie orgánov a agentúr Únie zapojených do politiky v oblasti kybernetickej bezpečnosti, ako je Európske centrum boja proti počítačovej kriminalite (EC3), Agentúra Európskej únie pre bezpečnosť letectva (EASA) a Agentúra Európskej únie pre vesmírny program (EUSPA), k účasti na jej práci.

(35) Príslušné orgány a jednotky CSIRT by mali mať možnosť zúčastňovať sa na výmenných programoch pre úradníkov z iných členských štátov s cieľom zlepšovať spoluprácu. Príslušné orgány by mali prijať potrebné opatrenia, ktoré úradníkom z iných členských štátov umožnia zohrávať účinnú úlohu v činnostiach hostiteľského príslušného orgánu.

(35a) 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 jej práci.

(36) [...]

(36a) S cieľom uľahčiť účinné vykonávanie ustanovení tejto smernice, napríklad pokiaľ ide o riadenie zraniteľností, riadenie kybernetickobezpečnostných rizík, opatrenia týkajúce sa oznamovania a dojednania o zdieľaní informácií, môžu členské štáty spolupracovať s tretími krajinami a vykonávať činnosti, ktoré sa považujú za vhodné na tento účel, vrátane výmeny informácií o hrozbách, incidentoch, zraniteľnostiach, nástrojoch a metódach, taktikách, technikách a postupoch, pripravenosti a cvičeniach v oblasti riadenia kybernetických kríz, odbornej príprave, budovaní dôvery a dojednaní o štruktúrovanom zdieľaní informácií. Takéto dohody o spolupráci by mali byť v súlade s právom Únie týkajúcim sa ochrany údajov.

(37) Členské štáty by mali prispieť k vytvoreniu rámca EÚ pre reakciu na kybernetické krízy stanoveného v odporúčaní (EÚ) 2017/1584 prostredníctvom existujúcich sietí spolupráce, najmä **Európskej** siete styčných organizácií pre kybernetické krízy (EU-CyCLONe), siete jednotiek CSIRT a skupiny pre spoluprácu. Sieť EU-CyCLONe a sieť jednotiek CSIRT by mali spolupracovať na základe procedurálnych opatrení, v ktorých sa vymedzujú podmienky spolupráce, **pričom by sa mali vyhnúť akejkoľvek duplicite úloh**. V rokovacom poriadku siete EU-CyCLONe by sa mali ďalej spresniť spôsoby fungovania siete, okrem iného vrátane úloh, spôsobov spolupráce, interakcií s inými relevantnými aktérmi a vzorových formulárov na zdieľanie informácií, ako aj komunikačných prostriedkov. Pokiaľ ide o krízové riadenie na **politickej** úrovni Únie, príslušné strany by sa mali opierať o integrované dojednania o politickej reakcii na krízu (IPCR). Komisia by mala na tento 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.

(37a) Sieť EU-CyCLONe by mala fungovať ako sprostredkovateľská sieť medzi technickou a politickou úrovňou počas kybernetickobezpečnostných incidentov a kríz veľkého rozsahu. Mala by posilniť spoluprácu na operačnej úrovni, pričom by mala vychádzať zo zistení siete jednotiek CSIRT a využívať vlastné kapacity na vypracovanie analýzy vplyvu incidentov a kríz veľkého rozsahu a podporovať rozhodovanie na politickej úrovni. Inštitúcie, orgány a agentúry EÚ by mali určiť príslušný orgán zodpovedný za riadenie bezpečnostných incidentov a kríz veľkého rozsahu, ktorý sa stane členom siete EU-CyCLONe.

(38) [...]

(39) [...]

(39a) Zodpovednosť za zaisťovanie bezpečnosti siete a informačného systému nesú vo veľkej miere kľúčové a dôležité subjekty. Mala by sa podporovať a rozvíjať kultúra riadenia rizika vrátane posúdenia rizika a vykonávania bezpečnostných opatrení primeraných existujúcim rizikám.

(40) Opatrenia na riadenie rizika by **mali zohľadňovať stupeň závislosti subjektu od sietí a informačných systémov a** mali by zahŕňať opatrenia na identifikáciu rizika incidentov, opatrenia na predchádzanie incidentom a ich odhaľovanie a zvládanie, ako aj opatrenia na zmiernenie ich vplyvu. Bezpečnosť sietí a informačných systémov by mala zahŕňať bezpečnosť uchovávaných, prenášaných a spracúvaných údajov.

(40a) Keďže ohrozenie bezpečnosti sietí a informačných systémov môže mať rôzny pôvod, v tejto smernici sa uplatňuje prístup „všetkých nebezpečenstiev“, ktorý zahŕňa ochranu sietí a informačných systémov a ich fyzického prostredia pred akoukoľvek udalosťou, ako je krádež, požiar, povodeň, zlyhanie telekomunikácie alebo výpadok elektrickej energie, alebo pred akýmkoľvek neoprávneným fyzickým prístupom, poškodením alebo zásahom v súvislosti s informáciami, ktorými subjekt disponuje, alebo zariadeniami na spracovanie informácií, ktoré by mohli ohroziť dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov. Opatrenia na riadenie rizík by sa preto mali zaoberať aj fyzickou a environmentálnou bezpečnosťou tým, že budú zahŕňať opatrenia na ochranu sietí a informačných systémov subjektu pred systémovými zlyhaniami, ľudskými chybami, zlomyseľným konaním alebo prírodnými javmi v súlade s európskymi alebo medzinárodne uznávanými normami, ako sú normy uvedené v sérii ISO 27000. V tejto súvislosti by sa subjekty mali v rámci svojich opatrení riadenia rizík zaoberať aj bezpečnosťou ľudských zdrojov a mali by mať zavedené vhodné postupy kontroly prístupu. Tieto opatrenia by mali byť v súlade so smernicou XXXX [smernica CER].

(40b) Ak nie sú k dispozícii vhodné európske systémy certifikácie kybernetickej bezpečnosti prijaté v súlade s nariadením (EÚ) 2019/881, členské štáty by mohli vyžadovať, aby subjekty používali certifikované produkty, služby a procesy IKT alebo aby získali certifikát v rámci dostupných vnútroštátnych systémov kybernetickej bezpečnosti na účely splnenia požiadaviek na riadenie kybernetickobezpečnostných rizík podľa tejto smernice.

(41) S cieľom vyhnúť sa neprimeranému finančnému a administratívnemu zaťaženiu kľúčových a dôležitých subjektov by požiadavky na riadenie kybernetickobezpečnostných rizík mali byť primerané riziku [...] **pre** danú sieť a daný informačný systém, berúc pritom do úvahy najnovší technický vývoj v oblasti takýchto opatrení a **náklady na ich vykonávanie. Náležitá pozornosť by sa mala venovať aj veľkosti subjektu, ako aj pravdepodobnosti výskytu incidentov a ich závažnosti.**

(41a) V záujme zmiernenia regulačného zaťaženia by požiadavky na vykonávanie opatrení na riadenie kybernetickobezpečnostných rizík stanovené pre stredné alebo malé subjekty alebo mikrosubjekty mali byť v zásade menej prísne, pokiaľ prísnejšie požiadavky nie sú odôvodnené na základe kritérií kritickosti alebo vnútroštátnych posúdení rizík, najmä pokiaľ ide o subjekty, ktoré spĺňajú kritériá súvisiace s kritickosťou stanovené v tejto smernici.

(42) 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 ich interní pracovníci IT alebo ktorých bezpečnosť zaisťujú externí dodávatelia. Požiadavky na riadenie kybernetickobezpečnostných rizík a na oznamovanie podľa tejto smernice by sa mali vzťahovať na príslušné kľúčové a dôležité subjekty bez ohľadu na to, či vykonávajú údržbu svojich sietí a informačných systémov interne alebo ju nechávajú vykonávať externe.

(42aa) Poskytovatelia služieb DNS, správcovia mien TLD a subjekty poskytujúce služby registrácie doménových mien pre TLD, poskytovatelia služieb cloud computingu, poskytovatelia služieb dátového centra, poskytovatelia siete na sprístupňovanie obsahu, poskytovatelia riadených služieb a poskytovatelia riadených bezpečnostných služieb by vzhľadom na svoj cezhraničný charakter mali podliehať vyššej miere harmonizácie na úrovni Únie. Vykonávanie kybernetickobezpečnostných opatrení by sa preto malo uľahčiť vykonávacím aktom.

(43) Riešenie kybernetickobezpečnostných rizík vyplývajúcich z dodávateľského reťazca subjektu a jeho vzťahu s dodávateľmi je obzvlášť dôležité vzhľadom na výskyt incidentov, keď sa subjekty stali obeťami kybernetických útokov a keď aktéri s nekalými úmyslami dokázali ohroziť bezpečnosť sietí a informačných systémov subjektu využívaním zraniteľností a zasiahnuť tak produkty a služby tretích strán. Subjekty by preto mali posúdiť a zohľadniť celkovú kvalitu produktov a postupy svojich dodávateľov a poskytovateľov služieb v oblasti kybernetickej bezpečnosti vrátane ich bezpečných vývojových postupov.

(44) Spomedzi poskytovateľov služieb zohrávajú poskytovatelia riadených bezpečnostných služieb (MSSP) osobitne dôležitú úlohu v pomoci subjektom v ich úsilí o odhaľovanie incidentov a reakciu na ne, a to v takých oblastiach, ako je reakcia na incidenty, penetračné testovanie, bezpečnostné audity a poradenstvo. Avšak aj samotní poskytovatelia MSSP boli cieľom kybernetických útokov a ich úzke zapojenie do činnosti prevádzkovateľov predstavuje osobitné kybernetickobezpečnostné riziko. Subjekty by preto mali výberu poskytovateľa MSSP venovať zvýšenú pozornosť.

(44a) Vnútroštátne príslušné orgány môžu v kontexte svojich úloh dohľadu využívať aj služby v oblasti kybernetickej bezpečnosti, ako sú bezpečnostné audity a penetračné testovanie alebo reakcia na incidenty. S cieľom pomôcť subjektom, ako aj vnútroštátnym príslušným orgánom pri výbere kvalifikovaných a dôveryhodných poskytovateľov služieb v oblasti kybernetickej bezpečnosti, by Komisia s pomocou skupiny pre spoluprácu a agentúry ENISA mala zvážiť možnosť požiadať o európske systémy certifikácie kybernetickej bezpečnosti v súlade s článkom 48 nariadenia (EÚ) 2019/881.

(45) Subjekty by mali riešiť aj kybernetickobezpečnostné riziká vyplývajúce z ich interakcií a vzťahov s inými zainteresovanými stranami v rámci širšieho ekosystému. Predovšetkým by 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 najmä o ochranu duševného vlastníctva. Podobne by subjekty, ktoré závisia od služieb v oblasti transformácie údajov a analýzy údajov od tretích strán, mali prijať všetky vhodné kybernetickobezpečnostné opatrenia, a to vzhľadom na význam a hodnotu údajov pre činnosti subjektov.

(46) V záujme ďalšieho riešenia rizík kľúčového dodávateľského reťazca a pomoci subjektom pôsobiacim v odvetviach, na ktoré sa vzťahuje táto smernica, pri náležitom riadení kybernetickobezpečnostných rizík súvisiacich s dodávateľským reťazcom a dodávateľmi, by skupina pre spoluprácu, do ktorej sú zapojené príslušné vnútroštátne orgány, mala v spolupráci s Komisiou a agentúrou ENISA vykonať koordinované odvetvové posúdenia rizík dodávateľského reťazca, ktoré sa už vykonali v prípade sietí 5G v nadväznosti na odporúčanie (EÚ) 2019/534 o kybernetickej bezpečnosti sietí 5G[21] s cieľom identifikovať za každé odvetvie kritické služby, systémy alebo produkty IKT, relevantné hrozby a zraniteľnosti.

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

(47) Pri posudzovaní rizík v dodávateľskom reťazci 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 celoeurópskom koordinovanom posúdení rizika 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 rizika, by sa mali zohľadniť tieto kritériá: i) rozsah, v akom kľúčové a dôležité subjekty využívajú konkrétne kritické služby, systémy alebo produkty IKT a spoliehajú sa na ne; ii) relevantnosť konkrétnych kritických služieb, systémov alebo produktov IKT pre vykonávanie kritických alebo citlivých funkcií vrátane spracúvania osobných údajov; iii) dostupnosť alternatívnych služieb, systémov alebo produktov IKT; iv) odolnosť celkového dodávateľského reťazca služieb, systémov alebo produktov IKT voči rušivým udalostiam a v) v prípade vznikajúcich služieb, systémov alebo produktov IKT ich potenciálny budúci význam pre činnosti subjektov.

(48) S cieľom zefektívniť právne 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 týmto subjektom a ich príslušným orgánom využívať právny rámec stanovený touto smernicou (vrátane určenia jednotky CSIRT zodpovednej za riešenie rizík a incidentov, účasť príslušných orgánov a subjektov na práci skupiny pre spoluprácu a siete jednotiek CSIRT), mali by sa tieto povinnosti zahrnúť do rozsahu pôsobnosti tejto smernice. Zodpovedajúce ustanovenia v nariadení Európskeho parlamentu a Rady (EÚ) č. 910/2014[22] a v smernici Európskeho parlamentu a Rady (EÚ) 2018/1972[23] týkajúce sa stanovenia požiadavky na bezpečnosť a oznamovanie pre tieto typy subjektov by sa preto mali zrušiť.

---

[22] 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).

[23] 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).

(48a) Povinnosti v oblasti bezpečnosti stanovené v tejto smernici by sa mali považovať za doplnkové k požiadavkám uloženým poskytovateľom dôveryhodných služieb podľa nariadenia (EÚ) č. 910/2014 (nariadenie eIDAS). 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 bezpečnostné incidenty podľa tejto smernice. Takéto povinnosti v oblasti bezpečnosti a oznamovania by sa mali týkať aj fyzickej ochrany poskytovanej služby. Naďalej sa uplatňuje článok 24 nariadenia (EÚ) č. 910/2014.

(48aa) Členské štáty môžu prideliť úlohu príslušných orgánov, pokiaľ ide o dôveryhodné služby, orgánom dohľadu eIDAS s cieľom zabezpečiť pokračovanie súčasných postupov a stavať na poznatkoch a skúsenostiach získaných pri uplatňovaní nariadenia eIDAS. Ak je táto úloha pridelená inému orgánu, vnútroštátne príslušné orgány podľa tejto smernice by mali úzko a včas spolupracovať formou výmeny relevantných informácií s cieľom zabezpečiť účinný dohľad a súlad poskytovateľov dôveryhodných služieb s požiadavkami stanovenými v tejto smernici a nariadení [XXXX/XXXX].

V náležitom prípade by vnútroštátny príslušný orgán podľa tejto smernice mal bezodkladne informovať orgán dohľadu eIDAS o každej oznámenej významnej kybernetickej hrozbe alebo incidente s dosahom na dôveryhodné služby, ako aj o akomkoľvek nesplnení požiadaviek podľa tejto smernice zo strany poskytovateľa dôveryhodných služieb. Na účely oznamovania môžu členské štáty prípadne použiť jednotný vstupný bod zriadený v záujme dosiahnutia spoločného a automatického oznamovania incidentov orgánu dohľadu eIDAS a tiež príslušnému orgánu podľa tejto smernice. Pravidlami týkajúcimi sa oznamovacích povinností by nemali byť dotknuté nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 a smernica Európskeho parlamentu a Rady 2002/58/ES[24].

---

[24] 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).

(49) V prípade potreby a s cieľom zabrániť zbytočnému narušeniu by sa existujúce vnútroštátne usmernenia [...] prijaté na účely transpozície pravidiel týkajúcich sa bezpečnostných opatrení stanovených v článkoch 40[...] a 41 smernice (EÚ) 2018/1972 [...] **mali zohľadniť v opatreniach týkajúcich sa transpozície, ktoré členské štáty vykonávajú v súvislosti s touto smernicou, čím sa bude stavať na znalostiach a zručnostiach doposiaľ nadobudnutých podľa smernice (EÚ) 2018/1972, pokiaľ ide o opatrenia na riadenie bezpečnostných rizík a oznámenia o incidentoch**. **Agentúra ENISA môže tiež vypracovať usmernenia zamerané na požiadavky týkajúce sa bezpečnosti a oznamovania určené poskytovateľom verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb s cieľom uľahčiť harmonizáciu, prechod a minimalizovať narušenie. Členské štáty môžu prideliť úlohu príslušných orgánov pre elektronické komunikácie národným regulačným orgánom s cieľom zabezpečiť pokračovanie súčasných postupov a stavať na poznatkoch a skúsenostiach získaných v smernici (EÚ) 2018/1972.**

(50) Vzhľadom na rastúci význam interpersonálnych komunikačných služieb nezávislých od číslovania je potrebné zabezpečiť, aby takéto služby tiež podliehali príslušným bezpečnostným požiadavkám vzhľadom na ich špecifický charakter a hospodársky význam. Poskytovatelia takýchto služieb by preto mali takisto zabezpečiť takú úroveň bezpečnosti sietí a informačných systémov, ktorá zodpovedá miere daného rizika. Vzhľadom na to, že poskytovatelia interpersonálnych komunikačných služieb nezávislých od číslovania obyčajne nevykonávajú samotnú kontrolu nad prenosom signálov v sieťach, stupeň rizika sa v prípade takýchto služieb môže v niektorých aspektoch považovať za nižší ako v prípade tradičných elektronických komunikačných služieb. To isté platí pre interpersonálne komunikačné služby, ktoré využívajú čísla a ktoré nevykonávajú skutočnú kontrolu nad prenosom signálu.

(51) Vnútorný trh je viac než kedykoľvek predtým závislý od fungovania internetu. Služby prakticky 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 verejné elektronické komunikačné siete, ako sú napríklad internetové chrbticové siete alebo podmorské komunikačné káble, mali zavedené vhodné kybernetickobezpečnostné opatrenia a aby oznamovali incidenty, ktoré sa ich týkajú.

(52) Ak je to **uplatniteľné**, [...] subjekty by mali informovať príjemcov svojich služieb o konkrétnych [...] opatreniach, ktoré môžu prijať na zmiernenie rizika, **ktoré im hrozí v dôsledku významnej kybernetickej hrozby**. **Subjekty by mali, ak je to vhodné, a najmä v prípadoch, keď sa môže naplniť významná kybernetická hrozba, informovať o samotnej hrozbe aj príjemcov svojich služieb spolu s príslušnými orgánmi alebo jednotkami CSIRT.** Požiadavka informovať týchto príjemcov o takýchto hrozbách by nemala subjekty zbaviť povinnosti na vlastné náklady prijať vhodné a okamžité opatrenia na prevenciu alebo odstránenie akýchkoľvek kybernetických hrozieb a obnovenie bežnej úrovne bezpečnosti služby. Takéto informácie o **kybernetických** [...] hrozbách by sa mali príjemcom poskytovať bezplatne.

(53) Poskytovatelia verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb by mali predovšetkým informovať príjemcov služieb o konkrétnych a významných kybernetických hrozbách a o opatreniach, ktoré môžu prijať na ochranu bezpečnosti svojej komunikácie, napríklad použitím určitých typov softvéru alebo šifrovacích technológií.

(54) S cieľom zaistiť bezpečnosť elektronických komunikačných sietí a služieb by sa malo podporovať používanie šifrovania, a najmä šifrovania medzi koncovými bodmi, a v prípade potreby by malo byť povinné pre poskytovateľov takýchto služieb a sietí v súlade so zásadami štandardnej a špecificky navrhnutej bezpečnosti a ochrany súkromia na účely článku 18. Používanie šifrovania medzi koncovými bodmi by sa malo zosúladiť s právomocami členských štátov na zabezpečenie ochrany ich základných bezpečnostných záujmov a verejnej bezpečnosti a na umožnenie vyšetrovania, odhaľovania a stíhania trestných činov v súlade s právom Únie. Riešenia na účely zákonného prístupu k informáciám v koncovej šifrovanej komunikácii by mali zachovať účinnosť šifrovania pri ochrane súkromia a bezpečnosti komunikácií a zároveň poskytovať účinnú reakciu na trestnú činnosť.

(55) V tejto smernici sa stanovuje dvojfázový prístup k oznamovaniu incidentov s cieľom nájsť správnu rovnováhu medzi rýchlym oznamovaním na jednej strane, ktoré pomáha zmierniť potenciálne šírenie incidentov a umožňuje subjektom hľadať podporu, a na druhej strane podávaním podrobných správ, v ktorých sa čerpajú cenné ponaučenia z jednotlivých incidentov a časom sa zlepšuje odolnosť jednotlivých podnikov a celých odvetví voči kybernetickým hrozbám. Ak sa subjekty dozvedia o incidente, malo by sa od nich vyžadovať, aby do 24 hodín predložili prvotné oznámenie, po ktorom bude najneskôr do jedného mesiaca nasledovať konečná správa. Prvotné oznámenie by malo obsahovať len informácie, ktoré sú nevyhnutne potrebné na to, aby sa príslušné orgány dozvedeli o incidente a v prípade potreby umožnili subjektu požiadať o pomoc. V takomto oznámení by sa prípadne malo uviesť, či je incident pravdepodobne spôsobený protiprávnym alebo zlomyseľným konaním. Členské štáty by mali zabezpečiť, aby požiadavka na predloženie tohto prvotného oznámenia neodklonila zdroje oznamujúceho subjektu od činností súvisiacich s riešením incidentov, ktoré by sa mali uprednostniť. S cieľom zabrániť tomu, aby sa z dôvodu povinností oznamovania incidentov odkláňali zdroje od riešenia reakcie na incidenty alebo aby sa inak ohrozilo úsilie subjektov v tejto súvislosti, by členské štáty mali takisto stanoviť, že v riadne odôvodnených prípadoch a po dohode s príslušnými orgánmi alebo jednotkami CSIRT sa dotknutý subjekt môže odchýliť od lehoty 24 hodín pre prvotné oznámenie a od lehoty jedného mesiaca pre záverečnú správu.

(55a) Proaktívny prístup ku kybernetickým hrozbám je základnou zložkou riadenia kybernetickobezpečnostných rizík, ktoré by malo príslušným orgánom umožniť účinne zabrániť tomu, aby sa z kybernetických hrozieb stali skutočné incidenty, ktoré by mohli spôsobiť značné materiálne alebo nemateriálne straty. Na tento účel je oznamovanie významných kybernetických hrozieb mimoriadne dôležité.

(56) Kľúčové a dôležité 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 záťaž a môžu viesť aj k nejasnostiam, pokiaľ ide o formát a postupy takéhoto oznamovania. Vzhľadom na to a na účely zjednodušenia oznamovania bezpečnostných incidentov by členské štáty [...] **mohli** zriadiť *jednotný vstupný bod* pre všetky oznámenia požadované podľa tejto smernice, ako aj podľa iných právnych predpisov Únie, ako napríklad nariadenie (EÚ) 2016/679 a smernica 2002/58/ES. Agentúra ENISA by spolu so skupinou pre spoluprácu mala vypracovať spoločné vzorové formuláre oznámení prostredníctvom usmernení, ktoré by zjednodušili a zefektívnili oznamovanie informácií požadovaných v právnych predpisoch Únie a znížili záťaž pre podniky.

(57) 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 centrum EC3 a agentúra ENISA uľahčili koordináciu medzi príslušnými orgánmi a orgánmi presadzovania práva jednotlivých členských štátov.

(58) V dôsledku incidentov je v mnohých prípadoch ohrozená ochrana osobných údajov. V tejto súvislosti by príslušné orgány mali spolupracovať a vymieňať si informácie o všetkých relevantných záležitostiach s orgánmi pre ochranu osobných údajov a dozornými orgánmi podľa smernice 2002/58/ES.

(59) Udržiavanie presných a úplných databáz doménových mien a registračných údajov (tzv. údajov 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 Únii. Ak spracúvanie zahŕňa osobné údaje, takéto spracúvanie musí byť v súlade s právnymi predpismi Únie o ochrane údajov.

(60) Dostupnosť a včasná prístupnosť týchto údajov pre orgány verejnej moci vrátane príslušných orgánov podľa práva Únie alebo vnútroštátneho práva na predchádzanie trestným činom, ich vyšetrovanie alebo stíhanie, pre jednotky CERT, jednotky CSIRT, a pokiaľ ide o údaje ich klientov pre poskytovateľov elektronických komunikačných sietí a služieb a poskytovateľov kybernetickobezpečnostných technológií a služieb konajúcich v mene týchto klientov, je nevyhnutná na predchádzanie zneužívaniu systému doménových mien a boj proti tomuto zneužívaniu, najmä na predchádzanie kybernetickobezpečnostným incidentom, ich odhaľovanie a reakciu na ne. Takýto prístup by mal byť v súlade s právnymi predpismi Únie o ochrane údajov, pokiaľ ide o osobné údaje.

(61) S cieľom zabezpečiť dostupnosť presných a úplných údajov o registrácii doménových mien by mali správcovia TLD a subjekty poskytujúce služby registrácie doménových mien pre TLD (tzv. registrátori) zhromažďovať registračné údaje o menách domén a zaručovať ich integritu a dostupnosť. **Pokiaľ ide o registračné údaje, subjekty by mali predovšetkým overiť meno a e-mailovú adresu držiteľa domény.** Správcovia TLD a subjekty poskytujúce služby registrácie doménových mien pre TLD by mali [...] stanoviť politiky a postupy na zhromažďovanie a uchovávanie presných a úplných registračných údajov, ako aj na predchádzanie nepresným registračným údajom a ich opravu v súlade s pravidlami Únie v oblasti ochrany údajov.

(62) Správcovia TLD a subjekty, ktoré pre nich poskytujú služby registrácie doménových mien, by mali zverejňovať registračné údaje o doménových menách, ktoré nepatria do rozsahu pôsobnosti pravidiel Únie v oblasti ochrany údajov, ako sú údaje, ktoré sa týkajú právnických osôb[25]. Správcovia TLD a subjekty poskytujúce služby registrácie doménových mien pre TLD by tiež mali oprávneným záujemcom o prístup umožniť zákonný prístup k špecifickým registračným údajom o doménových menách týkajúcim sa fyzických osôb v súlade s právnymi predpismi Únie o ochrane údajov. Členské štáty by mali zabezpečiť, aby správcovia TLD a subjekty, ktoré pre nich poskytujú služby registrácie doménových mien, bezodkladne reagovali na žiadosti [...] o zverejnenie registračných údajov o doménových menách podané **zo strany oprávnených záujemcov o prístup, ako sú príslušné orgány podľa práva Únie alebo vnútroštátneho práva v oblasti národnej bezpečnosti a trestnej justície alebo jednotky CSIRT.** Správcovia TLD a subjekty, ktoré pre nich poskytujú služby registrácie doménových mien, by mali stanoviť politiky a postupy uverejňovania a sprístupňovania registračných údajov vrátane dohôd o úrovni poskytovaných služieb na vybavovanie žiadostí o prístup od oprávnených záujemcov o prístup. Postup týkajúci sa udelenia prístupu môže zahŕňať aj použitie rozhrania, portálu alebo iného technického nástroja na zabezpečenie účinného systému na podávanie žiadostí o registračné údaje a prístup k nim. **Členské štáty by mali zabezpečiť, aby všetky typy prístupu k registračným údajom domény (osobným aj iným ako osobným údajom) boli bezplatné.** S cieľom podporovať harmonizované postupy na celom vnútornom trhu môže Komisia prijať usmernenia o takýchto postupoch bez toho, aby boli dotknuté právomoci Európskeho výboru pre ochranu údajov, **pričom tieto usmernenia budú v súlade s medzinárodnými normami vypracovanými komunitou viacerých zainteresovaných strán a budú tieto normy dopĺňať**.

---

[25] Odôvodnenie [...] 14 nariadenia [...] Európskeho parlamentu [...] a [...] Rady [...] (EÚ) 2016/679: „Toto nariadenie sa nevzťahuje na spracúvanie osobných údajov, ktoré sa týka právnických osôb, a najmä podnikov založených ako právnické osoby vrátane názvu, formy a kontaktných údajov právnickej osoby.“

(63) [...] **K**ľúčové a dôležité subjekty podľa tejto smernice by mali podliehať právomoci členského štátu, v ktorom poskytujú svoje služby. **Subjekty uvedené v bodoch 1 až 7 a 10 prílohy I, poskytovatelia dôveryhodných služieb a poskytovatelia internetových prepojovacích uzlov uvedení v bode 8 prílohy I a bodoch 1 až 5 prílohy II k tejto smernici by mali podliehať právomoci členského štátu, v ktorom sú usadené.** Ak subjekt poskytuje služby **alebo má miesto podnikateľskej činnosti** vo viac ako jednom členskom štáte, mal by podliehať samostatnej a súbežnej právomoci každého z týchto členských štátov. Príslušné orgány týchto členských štátov by mali spolupracovať, vzájomne si pomáhať a v prípade potreby vykonávať spoločné opatrenia dohľadu. **Ak sa členské štáty rozhodnú uplatniť svoju právomoc, mali by sa vyhnúť tomu, aby bolo rovnaké správanie sankcionované viac ako raz za porušenie povinností stanovených v tejto smernici.**

(64) S cieľom zohľadniť cezhraničný charakter služieb a operácií poskytovateľov služieb DNS, správcov mien TLD, **subjektov poskytujúcich služby registrácie doménových mien pre TLD**, poskytovateľov sietí na sprístupňovanie obsahu, poskytovateľov služieb cloud computingu, poskytovateľov služieb dátového centra a poskytovateľov digitálnych služieb by mal mať právomoc nad týmito subjektmi len jeden členský štát. Právomoc by sa mala udeliť členskému štátu, v ktorom má príslušný subjekt hlavné miesto podnikateľskej činnosti v Únii. Kritérium miesta podnikateľskej činnosti na účely tejto smernice zahŕňa účinné vykonávanie činnosti prostredníctvom stabilných dojednaní. Právna forma takýchto dojednaní, či už ide o pobočku alebo dcérsku spoločnosť s právnou subjektivitou, nie je v tomto ohľade určujúcim faktorom.

Spĺňanie tohto kritéria by nemalo závisieť od toho, či sa sieť a informačné systémy fyzicky nachádzajú na danom mieste; samotná prítomnosť a používanie takýchto systémov nepredstavuje hlavné miesto podnikateľskej činnosti, a preto nejde o rozhodujúce kritériá na určenie hlavného miesta podnikateľskej činnosti. Hlavným miestom podnikateľskej činnosti by malo byť miesto v Únii, kde sa **najčastejšie** prijímajú rozhodnutia týkajúce sa opatrení na riadenie kybernetickobezpečnostných rizík. Zvyčajne zodpovedá miestu ústredia spoločností v Únii. Ak **nie je možné určiť miesto, v ktorom sa takéto rozhodnutia prijímajú najčastejšie, alebo ak** sa takéto rozhodnutia neprijímajú v Únii, predpokladá sa, že hlavné miesto podnikateľskej činnosti je v členských štátoch, v ktorých majú subjekty miesto podnikateľskej činnosti s najvyšším počtom zamestnancov v Únii. Ak služby vykonáva skupina podnikov, hlavné miesto podnikateľskej činnosti riadiaceho podniku by sa malo považovať za hlavné miesto podnikateľskej činnosti skupiny podnikov.

(64a) Ak 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.

(64aa) S cieľom zabezpečiť jasný prehľad o poskytovateľoch služieb DNS, správcoch mien TLD, subjektoch poskytujúcich služby registrácie doménových mien pre TLD, poskytovateľoch sietí na sprístupňovanie obsahu, poskytovateľoch služieb cloud computingu, poskytovateľoch služieb dátového centra a poskytovateľoch digitálnych služieb, ktorí poskytujú služby v celej Únii v rozsahu pôsobnosti tejto smernice, by agentúra ENISA mala vytvoriť a viesť register pre takéto subjekty na základe oznámení doručených členským štátom, prípadne prostredníctvom ich vnútroštátnych mechanizmov na oznamovanie vlastných údajov. S cieľom zabezpečiť presnosť a úplnosť informácií, ktoré by sa mali zahrnúť do tohto registra, by členské štáty mali agentúre ENISA predkladať informácie o týchto subjektoch, ktoré sú dostupné v ich vnútroštátnych registroch. Agentúra ENISA a členské štáty by mali prijať opatrenia na uľahčenie interoperability takýchto registrov a zároveň zabezpečiť ochranu dôverných alebo utajovaných skutočností.

(65) V prípadoch, keď poskytovateľ služieb DNS, správca mien TLD, poskytovateľ siete na sprístupňovanie obsahu, poskytovateľ služieb cloud computingu, poskytovateľ služieb dátového centra a poskytovateľ digitálnych služieb, ktorí nie sú usadení v Únii, ponúkajú služby v rámci Únie, mal by sa určiť zástupca. Aby bolo možné určiť, či takýto subjekt ponúka služby v Únii, malo by sa zistiť, či je zrejmé, že daný subjekt plánuje ponúkať služby osobám v jednom alebo vo viacerých členských štátoch. Samotná dostupnosť webového sídla subjektu alebo jeho sprostredkovateľa v Únii alebo e-mailovej adresy a iných kontaktných údajov alebo použitie jazyka, ktorý sa všeobecne používa v tretej krajine, v ktorej je subjekt usadený, nepostačuje na potvrdenie takého úmyslu. Na základe faktorov, ako je používanie jazyka alebo meny bežne používaných v jednom alebo vo viacerých členských štátoch s možnosťou objednania služieb v tomto inom jazyku alebo zmienka o zákazníkoch alebo používateľoch, ktorí sa nachádzajú v Únii, môže byť však zjavné, že subjekt plánuje ponúkať služby v Únii. Zástupca by mal konať v mene subjektu a príslušné orgány alebo jednotky CSIRT by mali mať možnosť zástupcu kontaktovať. Subjekt by mal prostredníctvom písomného mandátu výslovne určiť zástupcu oprávneného konať v mene subjektu v súvislosti s jeho povinnosťami podľa tejto smernice vrátane oznamovania incidentov.

(66) Ak sa informácie, ktoré sa považujú za utajované podľa vnútroštátneho práva alebo práva Únie, vymieňajú, oznamujú alebo inak zdieľajú podľa ustanovení tejto smernice, mali by sa uplatňovať zodpovedajúce osobitné pravidlá zaobchádzania s utajovanými skutočnosťami.

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

(68) Subjekty by sa mali nabádať, aby kolektívne využívali svoje individuálne znalosti a praktické skúsenosti na strategickej, taktickej a operačnej úrovni s cieľom zlepšiť svoje schopnosti primerane posudzovať kybernetické hrozby, monitorovať ich, brániť sa proti nim a reagovať na ne. Preto treba umožniť, aby sa na úrovni Únie vytvorili mechanizmy dohôd o dobrovoľnom zdieľaní informácií. Na tento účel by členské štáty mali aktívne podporovať a podnecovať aj príslušné subjekty, na ktoré sa nevzťahuje rozsah pôsobnosti tejto smernice, aby sa na takýchto mechanizmoch zdieľania informácií zúčastňovali. Tieto mechanizmy by sa mali vykonávať v plnom súlade s pravidlami Únie týkajúcimi sa hospodárskej súťaže, ako aj právnymi predpismi Únie v oblasti ochrany údajov.

(69) [...] V rozsahu, ktorý je nevyhnutne potrebný a primeraný na účely zaistenia bezpečnosti sietí a informácií, **by sa spracúvanie osobných údajov kľúčovými a dôležitými** subjektmi [...] a poskytovateľmi bezpečnostných technológií a služieb **mohlo považovať za nevyhnutné na splnenie zákonnej povinnosti alebo** [...] by mohlo predstavovať oprávnený záujem dotknutého prevádzkovateľa **[...]**, ako sa uvádza v nariadení (EÚ) 2016/679. To by **mohlo** [...] zahŕňať opatrenia týkajúce sa prevencie, odhaľovania a analýzy incidentov a reakcie na ne, opatrenia na zvýšenie informovanosti o konkrétnych kybernetických hrozbách, výmenu informácií v kontexte nápravy zraniteľnosti a koordinovaného zverejňovania, ako aj dobrovoľnú výmenu informácií o týchto incidentoch, [...] kybernetických hrozbách a zraniteľnostiach, ukazovatele kompromitácie, taktiky, techniky a postupy, kybernetickobezpečnostné varovania a konfiguračné nástroje. Takéto opatrenia si môžu vyžadovať spracovanie [...] **rôznych** druhov osobných údajov, **ako sú**: IP adresy, jednotné vyhľadávače prostriedkov (URL), doménové mená a e-mailové adresy. **Spracúvanie osobných údajov príslušnými orgánmi, jednotnými kontaktnými miestami a jednotkami CSIRT by sa malo stanoviť vo vnútroštátnom práve a malo by sa považovať za nevyhnutné na splnenie zákonnej povinnosti alebo na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi, ako sa uvádza v článku 6 ods. 1 písm. c) alebo e) nariadenia (EÚ) 2016/679.**

(69a) V právnych predpisoch členských štátov sa môžu stanoviť pravidlá, ktoré príslušným orgánom, jednotným kontaktným miestam a jednotkám CSIRT v rozsahu, ktorý je nevyhnutne potrebný a primeraný na účely zaistenia bezpečnosti sietí a informačných systémov kľúčových a dôležitých subjektov, umožnia spracúvať osobitné kategórie osobných údajov v súlade s článkom 9 [...] nariadenia (EÚ) 2016/679, a to najmä stanovením vhodných a konkrétnych opatrení na ochranu základných práv a záujmov fyzických osôb vrátane technických obmedzení týkajúcich sa opätovného používania takýchto údajov a používania špičkových opatrení v oblasti bezpečnosti a ochrany súkromia, ako je pseudonymizácia alebo šifrovanie, v prípade, ak anonymizácia môže výrazne ovplyvniť sledovaný účel.

(70) 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 medzi kľúčovými a dôležitými subjektmi s cieľom zabezpečiť spravodlivú rovnováhu povinností pre subjekty aj príslušné orgány. Kľúčové subjekty by preto mali podliehať plnohodnotnému režimu dohľadu (*ex ante* a *ex post*), zatiaľ čo na dôležité subjekty by sa mal vzťahovať zjednodušený režim dohľadu, a to len *ex post*. V druhom prípade to znamená, že od dôležitých subjektov **by sa nemalo vyžadovať, aby** [...] systematicky **dokumentovali** súlad s požiadavkami na riadenie kybernetickobezpečnostných rizík, zatiaľ čo príslušné orgány by mali k dohľadu uplatňovať reaktívny prístup *ex post*, a preto by nemali mať všeobecnú povinnosť vykonávať nad týmito subjektmi dohľad. **V prípade dôležitých subjektov sa dohľad *ex post* môže spustiť na základe dôkazov alebo akýchkoľvek náznakov alebo informácií, na ktoré boli upozornené príslušné orgány a ktoré tieto orgány považujú za potenciálne nedodržiavanie povinností stanovených v tejto smernici. Takéto dôkazy, náznaky alebo informácie môžu byť napríklad takého druhu, aký príslušným orgánom poskytujú iné orgány, subjekty, občania, médiá alebo iné zdroje, verejne dostupné informácie, alebo môžu vyplývať z iných činností, ktoré príslušné orgány vykonávajú pri plnení svojich úloh.**

(70a) Pri vykonávaní dohľadu *ex ante* by príslušné orgány mali mať možnosť primeraným spôsobom rozhodnúť o uprednostňovaní použitia opatrení a prostriedkov v oblasti dohľadu, ktoré majú k dispozícii. To znamená, že príslušné orgány môžu rozhodnúť o uprednostňovaní 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 rizika a zodpovedajúce opatrenia a prostriedky v oblasti dohľadu odporúčané pre jednotlivé kategórie rizika, ako je použitie, frekvencia alebo typ kontrol na mieste alebo cielených bezpečnostných auditov alebo bezpečnostných kontrol, druh informácií, ktoré sa majú vyžadovať, a úroveň podrobnosti týchto informácií. Takéto metodiky dohľadu môžu 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.

(70aa) V súvislosti so subjektmi verejnej správy by sa právomoci v oblasti dohľadu mali vykonávať v súlade s vnútroštátnymi rámcami a právnym poriadkom. Členské štáty by mali mať možnosť rozhodnúť o uložení vhodných, primeraných a účinných opatrení dohľadu a presadzovania vo vzťahu k týmto subjektom.

(70aaa) S cieľom preukázať súlad s určitými opatreniami na riadenie kybernetickobezpečnostných rizík by členské štáty mohli od kľúčových a dôležitých subjektov vyžadovať, aby používali kvalifikované dôveryhodné služby alebo oznámené schémy elektronickej identifikácie podľa nariadenia (EÚ) č. 910/2014.

(71) Aby bolo presadzovanie povinností účinné, mal by sa stanoviť minimálny zoznam správnych sankcií za porušenie povinností v oblasti riadenia kybernetickobezpečnostných rizík a oznamovania stanovených v tejto smernici, ktorým sa stanoví jasný a konzistentný rámec pre takéto sankcie v celej Únii. Náležitá pozornosť by sa mala venovať povahe, závažnosti a trvaniu porušenia, skutočnej spôsobenej škode alebo vzniknutým stratám alebo potenciálnym škodám či stratám, ktoré mohli vzniknúť, úmyselnému alebo nedbanlivostnému charakteru porušenia, opatreniam prijatým na zabránenie alebo zmiernenie vzniknutej škody a/alebo strát, miere zodpovednosti alebo akémukoľvek relevantnému predchádzajúcemu porušeniu, miere spolupráce s príslušným orgánom a akýmkoľvek ďalším priťažujúcim alebo poľahčujúcim faktorom. Ukladanie sankcií vrátane správnych pokút by malo podliehať primeraným procesným zárukám v súlade so všeobecnými zásadami práva Únie a Charty základných práv Európskej únie vrátane účinnej súdnej ochrany a riadneho procesu.

(71a) Ustanovenia týkajúce sa zodpovednosti fyzických osôb, ktoré majú určitú zodpovednosť v rámci subjektu, za porušenie ich úlohy zabezpečovať dodržiavanie povinností stanovených v tejto smernici nevyžadujú od členských štátov, aby zabezpečili trestné stíhanie alebo občianskoprávnu zodpovednosť za škody spôsobené takýmto porušením voči tretím stranám.

(72) 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.

(73) Keď sa správne pokuty ukladajú podniku, podnik by sa mal na tieto účely považovať za podnik v súlade s článkami 101 a 102 ZFEÚ. Ak sa správne pokuty ukladajú osobám, ktoré nie sú podnikom, dozorný 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 príslušnými orgánmi alebo iných sankcií stanovených vo vnútroštátnych predpisoch, ktorými sa transponuje táto smernica.

(74) Členské štáty [...] **môžu** 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.

(75) 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 povinností stanovených v tejto smernici. Povaha týchto sankcií, trestná alebo správna, by sa mala určiť v právnom predpise členského štátu.

(76) S cieľom ďalej posilniť účinnosť a odrádzajúci účinok sankcií za porušenie povinností stanovených podľa tejto smernice by príslušné orgány mali byť oprávnené uplatňovať sankcie pozostávajúce z pozastavenia certifikácie alebo povolenia časti alebo všetkých služieb, ktoré poskytuje kľúčový subjekt, a uloženia dočasného zákazu fyzickej osobe vykonávať riadiace funkcie. Takéto sankcie by sa vzhľadom na svoju závažnosť a vplyv na činnosti subjektov a v konečnom dôsledku na ich spotrebiteľov mali uplatňovať len úmerne k závažnosti porušenia a s prihliadnutím na osobitné okolnosti každého prípadu vrátane úmyselného alebo nedbanlivostného charakteru porušenia, opatrení prijatých na zabránenie alebo zmiernenie vzniknutej škody a/alebo strát. Takéto sankcie by sa mali uplatňovať len ako ultima ratio, čo znamená až po vyčerpaní ostatných príslušných opatrení na presadzovanie povinností stanovených v tejto smernici, a len na obdobie, kým subjekty, na ktoré sa vzťahujú, neprijmú potrebné opatrenia na nápravu nedostatkov alebo na splnenie požiadaviek príslušného orgánu, v prípade ktorých sa takéto sankcie uplatnili. Ukladanie takýchto sankcií by malo podliehať primeraným procesným zárukám v súlade so všeobecnými zásadami práva Únie a Charty základných práv Európskej únie vrátane účinnej súdnej ochrany, riadneho procesu, prezumpcie neviny a práva na obhajobu.

(76a) S cieľom zabezpečiť účinný dohľad a presadzovanie, najmä v prípadoch s cezhraničným rozmerom, by členské štáty, ktorým bola doručená žiadosť o vzájomnú pomoc, mali v rozsahu žiadosti prijať primerané opatrenia v oblasti dohľadu a presadzovania vo vzťahu k dotknutému subjektu, ktorý poskytuje služby alebo ktorý má sieť a informačný systém na ich území.

(77) Touto smernicou by sa mali stanoviť pravidlá spolupráce medzi príslušnými orgánmi a dozornými orgánmi v súlade s nariadením (EÚ) 2016/679 s cieľom riešiť porušenia týkajúce sa osobných údajov.

(78) Cieľom tejto smernice by malo byť zabezpečenie vysokej úrovne zodpovednosti za opatrenia v oblasti riadenia kybernetickobezpečnostných rizík a oznamovacích povinností na úrovni organizácií. Z týchto dôvodov by riadiace orgány subjektov, ktoré patria do rozsahu pôsobnosti tejto smernice, mali schvaľovať opatrenia v oblasti kybernetickobezpečnostných rizík a dohliadať na ich vykonávanie.

(79) Mal by sa zaviesť **systém** partnerského [...] **zisťovania** [...], **ktorý by pomohol posilniť vzájomnú** dôveru a **poučiť sa z osvedčených postupov a skúseností**, čo by umožnilo [...] **partnerské výmeny informácií** zo strany odborníkov určených členskými štátmi, **pokiaľ ide o** [...] vykonávanie politík v oblasti kybernetickej bezpečnosti. **Pri vykonávaní systému partnerského zisťovania by sa mala osobitná pozornosť venovať tomu, aby sa zabezpečilo, že nebude zbytočne alebo neprimerane zaťažovať príslušné orgány členských štátov. Komisia by mala preskúmať všetky možnosti, ako potenciálne zaručiť finančné krytie nákladov, ktoré môžu vyplynúť z organizovania misií zameraných na partnerské zisťovanie. Systém partnerského zisťovania by mal okrem toho zohľadňovať výsledky podobných mechanizmov, ako je systém partnerského preskúmania siete jednotiek CSIRT, prinášať pridanú hodnotu a vyhýbať sa duplicite. Vykonávaním systému partnerského zisťovania by nemali byť dotknuté vnútroštátne ani únijné právne predpisy o ochrane dôverných a utajovaných skutočností. Pred začatím kôl partnerského zisťovania môžu členské štáty vykonať sebahodnotenie príslušných aspektov. Na žiadosť skupiny pre spoluprácu môže agentúra ENISA v prípade potreby poskytnúť usmernenia týkajúce sa sebahodnotenia a príslušných vzorových formulárov. Členské štáty by mali mať možnosť rozhodnúť, že svoje správy sprístupnia verejnosti.**

(80) [...]

(81) S cieľom zabezpečiť jednotné podmienky vykonávania príslušných ustanovení tejto smernice týkajúcich sa procedurálnych opatrení potrebných na fungovanie skupiny pre spoluprácu, technických prvkov týkajúcich sa opatrení na riadenie rizík alebo druhu informácií, formátu a postupu oznamovania incidentov, **kategórií subjektov, od ktorých by sa malo vyžadovať používanie určitých certifikovaných produktov, služieb a procesov IKT,** by sa mali na Komisiu preniesť vykonávacie právomoci. Uvedené právomoci by sa mali vykonávať v súlade s nariadením Európskeho parlamentu a Rady (EÚ) č. 182/2011[26].

(82) Komisia by mala túto smernicu pravidelne preskúmavať a radiť sa pritom so zainteresovanými subjektmi najmä s cieľom určiť, či ju treba zmeniť na základe zmien spoločenských, politických, technologických alebo trhových podmienok.

[26] 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).

(83) Keďže cieľ tejto smernice, a to dosiahnutie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, nie je možné uspokojivo dosiahnuť na úrovni samotných členských štátov, ale z dôvodu účinku tohto opatrenia 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.

(84) V tejto smernici sa dodržiavajú základné práva a zásady uznané Chartou základných práv Európskej únie, najmä právo na rešpektovanie súkromného života a komunikácie, ochrana osobných údajov, sloboda podnikania, právo vlastniť majetok, právo na účinný prostriedok nápravy pred súdom a právo na vypočutie. Táto smernica by sa mala vykonávať v súlade s uvedenými právami a zásadami,

PRIJALI TÚTO SMERNICU:

KAPITOLA I

Všeobecné ustanovenia

Článok 1

Predmet úpravy

1. Touto smernicou sa stanovujú opatrenia na zaistenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii **s cieľom zlepšiť fungovanie vnútorného trhu**.

2. Na tento účel sa v tejto smernici:

   a) stanovujú povinnosti členských štátov prijať národné stratégie kybernetickej bezpečnosti, určiť príslušné vnútroštátne orgány, jednotné kontaktné miesta a jednotky pre riešenie počítačových bezpečnostných incidentov (CSIRT);

   b) stanovujú pre subjekty typu uvedeného [...] v prílohách **I a II** povinnosti riadenia kybernetickobezpečnostných rizík a ich oznamovania[...];

   c) stanovujú **pravidlá a** povinnosti týkajúce sa zdieľania informácií o kybernetickej bezpečnosti.

Článok 2

Rozsah pôsobnosti

1. Táto smernica sa vzťahuje na verejné a súkromné subjekty typu **uvedeného** [...] v [...] prílohách **I a II** [...]**, ktoré spĺňajú alebo prekračujú limity pre stredné podniky** [...] v zmysle odporúčania Komisie 2003/361/ES[27]. **Článok 3 ods. 4 a článok 6 ods. 2 druhý a tretí pododsek prílohy k uvedenému odporúčaniu sa na účely tejto smernice neuplatňujú.**

2. [...]**B**ez ohľadu na [...]veľkosť **subjektov uvedených v odseku 1** sa táto smernica uplatňuje, aj **ak**: [...]

   a) služby poskytuje jeden z týchto subjektov:

      i) **poskytovatelia** verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb uvedení v bode 8 prílohy I;

      ii) **kvalifikovaní poskytovatelia dôveryhodných služieb uvedení v bode XX prílohy I;**

      iii) **nekvalifikovaní poskytovatelia dôveryhodných služieb uvedení v bode XX prílohy I;**

      iv) správcovia mien domény najvyššej úrovne a [...] uvedení v bode 8 prílohy I;

   b) [...]

---

27 Odporúčanie Komisie 2003/361/ES zo 6. mája 2003 o vymedzení pojmov mikro, malé a stredné podniky (Ú. v. EÚ L 124, 20.5.2003, s. 36).

c) je subjekt v **členskom štáte** jediným poskytovateľom služby, [...] **ktorá je kľúčová pre zachovanie kritických spoločenských alebo hospodárskych činností;**

d) potenciálne narušenie služby poskytovanej subjektom by mohlo mať [...] **významný** vplyv na ochranu verejnosti, verejnú bezpečnosť alebo verejné zdravie;

e) potenciálne narušenie služby poskytovanej subjektom by mohlo vyvolať [...] **významné** systémové riziká, najmä v odvetviach, v ktorých by takéto narušenie mohlo mať cezhraničný vplyv;

f) [...];

g) subjekt je identifikovaný ako kritický subjekt podľa smernice Európskeho parlamentu a Rady (EÚ) XXXX/XXXX[28] [smernica o odolnosti kritických subjektov] alebo ako subjekt rovnocenný s kritickým subjektom podľa článku 7 uvedenej smernice.

2a. **Táto smernica sa vzťahuje aj na subjekty verejnej správy na úrovni ústrednej štátnej správy uznané ako také v členskom štáte v súlade s vnútroštátnym právom a uvedené v bode 9 prílohy I, a to bez ohľadu na ich veľkosť. Členské štáty môžu ustanoviť, že sa táto smernica vzťahuje aj na subjekty verejnej správy na regionálnej a miestnej úrovni.**

28 [vložte celý názov a odkaz na uverejnenie v Ú. v., keď budú známe]

3. [...]

Touto smernicou nie sú dotknuté povinnosti členských štátov chrániť národnú bezpečnosť ani ich právomoc chrániť iné základné funkcie štátu vrátane zabezpečenia územnej celistvosti štátu a udržiavania verejného poriadku.

3a. 1. Táto smernica sa nevzťahuje na:

a) subjekty, ktoré nepatria do rozsahu pôsobnosti práva Únie, a v každom prípade všetky subjekty, ktoré primárne vykonávajú činnosti v oblasti obrany, národnej bezpečnosti, verejnej bezpečnosti alebo presadzovania práva, bez ohľadu na to, ktorý subjekt vykonáva tieto činnosti, a či ide o verejný subjekt alebo súkromný subjekt, bez toho, aby bol dotknutý bod 2;

b) subjekty, ktoré vykonávajú činnosti v oblasti súdnictva, parlamenty alebo centrálne banky.[...]

2. Ak subjekty verejnej správy vykonávajú činnosti v týchto oblastiach len ako súčasť svojich celkových činností, vylúčia sa z rozsahu pôsobnosti tejto smernice úplne.

3aa. Táto smernica sa nevzťahuje na:

i) činnosti subjektov, ktoré nepatria do rozsahu pôsobnosti práva Únie, a v každom prípade všetky činnosti v oblasti obrany alebo národnej bezpečnosti, bez ohľadu na to, ktorý subjekt vykonáva tieto činnosti, a či ide o verejný subjekt alebo súkromný subjekt;

ii) činnosti subjektov v súdnictve, parlamenty, centrálne banky a v oblasti verejnej bezpečnosti vrátane subjektov verejnej správy vykonávajúcich činnosti v oblasti presadzovania práva na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií.

3aaa. Povinnosti ustanovené v tejto smernici nezahŕňajú poskytovanie informácií, ktorých zverejnenie je v rozpore so základnými záujmami členských štátov v oblasti národnej bezpečnosti, verejnej bezpečnosti alebo obrany.

3aaaa. Touto smernicou nie je dotknuté právo Únie týkajúce sa ochrany osobných údajov, predovšetkým nariadenie (EÚ) 2016/679 a smernica 2002/58/ES.

3b. Táto smernica sa nevzťahuje na subjekty, ktoré sú vyňaté z pôsobnosti nariadenia Európskeho parlamentu a Rady (EÚ) XXXX/XXXX [nariadenie o digitálnej prevádzkovej odolnosti finančných služieb (DORA)] v súlade s jeho článkom 2 ods. 4.

4. Uplatňovaním tejto smernice nie sú dotknuté [...][29] [...] smernice Európskeho parlamentu a Rady 2011/93/EÚ[30] a 2013/40/EÚ[31].

5. Bez toho, aby bol dotknutý článok 346 ZFEÚ, informácie, ktoré sú dôverné podľa predpisov Únie a vnútroštátnych predpisov, ako napríklad predpisov o obchodnom tajomstve, sa vymieňajú s Komisiou a inými príslušnými orgánmi **v súlade s touto smernicou** len v prípade, ak je takáto výmena potrebná na účely uplatňovania tejto smernice. Vymieňané informácie sa obmedzujú na také informácie, ktoré sú relevantné a primerané účelu takejto výmeny. Pri výmene informácií sa zachováva dôvernosť týchto informácií a chránia sa bezpečnostné a obchodné záujmy kľúčových alebo dôležitých subjektov.

---

29 [...]

30 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).

31 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).

Článok 2a

Kľúčové a dôležité subjekty

1. Zo subjektov, na ktoré sa vzťahuje táto smernica, sa za kľúčové subjekty považujú:

i) subjekty typu ustanoveného v bodoch 1 až 8a a 10 prílohy I k tejto smernici, ktoré prekračujú limity pre stredné podniky vymedzené v odporúčaní Komisie 2003/361/ES;

ii) stredne veľké subjekty uvedené v článku 2 ods. 2 písm. a) bode i);

iii) subjekty uvedené v článku 2 ods. 2 písm. a) bodoch ii) a iv) tejto smernice bez ohľadu na veľkosť;

iv) subjekty uvedené v článku 2 ods. 2 písm. g) a v článku 2 ods. 2a tejto smernice bez ohľadu na veľkosť;

v) subjekty, ktoré členské štáty označili pred nadobudnutím účinnosti tejto smernice ako prevádzkovateľov základných služieb v súlade so smernicou (EÚ) 2016/1148 alebo s vnútroštátnym právom, ak tieto subjekty zriadili samotné členské štáty;

vi) subjekty typu ustanoveného v prílohy II, ktoré prekračujú limity pre stredné podniky vymedzené v odporúčaní Komisie 2003/361/ES a ktoré členské štáty označia za kľúčové na základe kritérií uvedených v článku 2 ods. 2 písm. c) až e);

vii) subjekty strednej veľkosti v zmysle odporúčania Komisie 2003/361/ES, ktoré členské štáty označia za kľúčové na základe kritérií uvedených v článku 2 ods. 2 písm. c) až e);

viii) mikro alebo malé subjekty v zmysle odporúčania Komisie 2003/361/ES ustanovené v odseku 2 písm. a) bode i) alebo označené podľa odseku 2 písm. c) až e) tohto článku, ktoré členské štáty označia za kľúčové na základe vnútroštátnych posúdení rizík.

2. Zo subjektov, na ktoré sa vzťahuje táto smernica, sa za dôležité subjekty považujú:

i) subjekty typu ustanoveného v prílohe I k tejto smernici, ktoré spĺňajú podmienky stredných podnikov v zmysle odporúčania Komisie 2003/361/ES a subjekty typu ustanoveného v prílohe II, ktoré spĺňajú alebo prekračujú limity pre stredné podniky v zmysle odporúčania Komisie 2003/361/ES[32];

ii) subjekty uvedené v článku 2 ods. 2 písm. a) bode iii) tejto smernice bez ohľadu na veľkosť;

iii) malé subjekty a mikrosubjekty uvedené v článku 2 ods. 2 písm. a) bode i);

iv) malé subjekty a mikrosubjekty, ktoré členské štáty označia za dôležité subjekty na základe článku 2 ods. 2 písm. c) až e).

[32] Odporúčanie Komisie 2003/361/ES zo 6. mája 2003 o vymedzení pojmov mikro, malé a stredné podniky (Ú. v. EÚ L 124, 20.5.2003, s. 36).

Článok 2a

Oznamovacie mechanizmy

1. **Členské štáty môžu zaviesť vnútroštátny mechanizmus oznamovania vlastných údajov, ktorým sa od všetkých subjektov, ktoré patria do rozsahu pôsobnosti tejto smernice vyžaduje, aby príslušným orgánom podľa tejto smernice alebo orgánom, ktoré na tento účel určia členské štáty, oznámili aspoň svoj názov, adresu, kontaktné údaje, odvetvie, v ktorom pôsobia, alebo druh služby, ktorú poskytujú, a prípadne zoznam členských štátov, v ktorých poskytujú služby, na ktoré sa vzťahuje táto smernica.**

2. Členské štáty v súvislosti [...] **so subjektmi, ktoré určili podľa článku 2 ods. 2 písm. b) až e),** oznamujú Komisii **aspoň relevantné informácie o počte určených subjektov, odvetvia, do ktorého patria, alebo druhu služieb, ktoré poskytujú, ako sa uvádza v prílohách, a konkrétne ustanovenie alebo ustanovenia článku 2 ods. 2, na základe ktorých boli určené do [12 mesiacov po lehote na transpozíciu tejto smernice].** Členské štáty [...] **tieto informácie** [...] následne pravidelne preskúmavajú, a to aspoň každé dva roky, a v prípade potreby ich aktualizujú.

Článok 2b

Akty Únie platné pre jednotlivé odvetvia

1. Ak sa v [...] **právnych** aktoch **Únie** [...] platných pre jednotlivé odvetvia vyžaduje, aby kľúčové alebo dôležité subjekty buď [...] prijali opatrenia na riadenie kybernetickobezpečnostných rizík, alebo aby oznamovali **významné** incidenty alebo [...] kybernetické hrozby, 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 VI** sa na **takéto subjekty** nevzťahujú. **Ak sa právne akty Únie platné pre jednotlivé odvetvia nevzťahujú na všetky subjekty v konkrétnom odvetví, ktoré patria do rozsahu pôsobnosti tejto smernice, na subjekty, na ktoré sa takéto ustanovenia pre jednotlivé odvetvia nevzťahujú, sa príslušné ustanovenia tejto smernice naďalej uplatňujú.**

2. Požiadavky uvedené v odseku 1 tohto článku sa považujú za požiadavky, ktorých účinky sú rovnocenné s účinkami povinností stanovenými v tejto smernici, ak sa v príslušnom akte Únie platnom pre dané odvetvie ustanovuje okamžitý, v prípade potreby automatický a priamy prístup k oznámeniam o incidentoch zo strany príslušných orgánov podľa tejto smernice alebo určených jednotiek CSIRT, a ak:

a) opatrenia na riadenie kybernetickobezpečnostných rizík majú aspoň rovnaký účinok ako opatrenia stanovené v článku 18 ods. 1 a 2 tejto smernice alebo

b) požiadavky na oznamovanie významných incidentov majú aspoň rovnaký účinok ako opatrenia stanovené v článku 20 ods. 1 až 6 tejto smernice.

3. Komisia pravidelne preskúmava uplatňovanie požiadaviek na rovnocenný účinok stanovených v odsekoch 1 a 2 tohto článku vo vzťahu k ustanoveniam právnych aktov Únie platných pre jednotlivé odvetvia. Komisia pri príprave týchto pravidelných preskúmaní konzultuje so skupinou pre spoluprácu a agentúrou ENISA.

Článok 3

Minimálna harmonizácia

Členské štáty môžu[...] bez toho, aby boli dotknuté ich povinnosti podľa práva Únie, prijať alebo zachovať ustanovenia na dosiahnutie vyššej úrovne kybernetickej bezpečnosti v **oblastiach, na ktoré sa vzťahuje táto smernica**.

Článok 4

Vymedzenie pojmov

Na účely tejto smernice sa uplatňuje toto vymedzenie pojmov:

1. „sieť a informačný systém“ je:

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

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

   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;

2a. „elektronická komunikačná služba“ je elektronická[...] komunikačná služba v zmysle článku 2 bodu 4 smernice (EÚ) 2018/1972;

3. „kybernetická bezpečnosť“ je kybernetická bezpečnosť v zmysle článku 2 bodu 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881[33];

4. „národná stratégia **kybernetickej bezpečnosti**“ [...] je súdržný rámec členského štátu, ktorým sa zabezpečuje riadenie s cieľom dosiahnuť strategické ciele a priority v **oblasti** [...] **kybernetickej bezpečnosti** [...] v danom členskom štáte;

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

5a. „rozsiahly kybernetickobezpečnostný incident“ je incident s významným vplyvom na najmenej dva členské štáty alebo incident, ktorý spôsobí narušenie, ktoré presahuje schopnosť členského štátu reagovať naň.

---

33 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).

6. „riešenie incidentov“ sú všetky kroky a postupy zamerané na odhaľovanie, analýzu a obmedzovanie následkov incidentu a reakcie naň;

6a. „riziko“ je potenciál straty alebo narušenia v dôsledku incidentu a vyjadruje sa ako kombinácia rozsahu takejto straty alebo narušenia a pravdepodobnosti výskytu daného incidentu;

7. „kybernetická hrozba“ je kybernetická hrozba v zmysle článku 2 bodu 8 nariadenia (EÚ) 2019/881;

7a. **„významná kybernetická hrozba“ je kybernetická hrozba, o ktorej možno na základe jej technických vlastností predpokladať, že má potenciál závažne ovplyvniť sieť a informačné systémy subjektu alebo jeho používateľov tým, že spôsobí značné hmotné alebo nehmotné straty;**

8. „zraniteľnosť“ je slabé miesto, náchylnosť alebo chyba aktíva IKT alebo systému, [...] ktoré môžu byť zneužité kybernetickou hrozbou;

8a. „odvrátená udalosť“ je udalosť, ktorá mala potenciál poškodiť sieť a informačné systémy subjektu alebo jeho používateľov, ale ktorej sa úspešne zabránilo prejaviť sa v plnej miere;

9. „zástupca“ je každá fyzická alebo právnická osoba usadená v Únii, ktorá je výslovne určená konať v mene i) poskytovateľa služieb DNS, správcu mien domény najvyššej úrovne (TLD), poskytovateľa služieb cloud computingu, poskytovateľa služieb dátových centier, poskytovateľa siete na sprístupňovanie obsahu podľa bodu 8 prílohy I alebo ii) subjektov uvedených v bode [...] **6** prílohy II, ktoré nie sú usadené v Únii, a vnútroštátny príslušný orgán alebo jednotka CSIRT sa môžu na túto osobu obracať namiesto subjektu, pokiaľ ide o povinnosti daného subjektu podľa tejto smernice;

10. „norma“ je norma v zmysle článku 2 bodu 1 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1025/2012[34];

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

12. „internetový prepojovací uzol (IXP)“ je sieťové zariadenie, ktoré umožňuje prepojenie viac než dvoch nezávislých sietí (autonómnych systémov), najmä na účely uľahčenia internetového dátového toku; IXP prepojuje len autonómne systémy; pri IXP nemusí internetový dátový tok medzi ktoroukoľvek dvojicou zúčastnených autonómnych systémov prechádzať cez žiadny tretí autonómny systém, pričom tento dátový tok sa nijako nemení ani sa doň nijako nezasahuje;

13. „systém doménových mien (DNS)“ je hierarchický distribuovaný systém pomenovaní, ktorý umožňuje koncovým používateľom dostať sa k službám a zdrojom na internete;

14. „poskytovateľ služieb DNS“ je subjekt, ktorý poskytuje služby rekurzívneho alebo autoritatívneho rozlišovania doménových mien **pre** [...] **použitie tretími stranami s výnimkou koreňových menných serverov** [...];

---

34 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).

15. „správca mien domény najvyššej úrovne“ je subjekt, ktorému bola udelená osobitná doména najvyššej úrovne (TLD) a ktorý je zodpovedný za správu TLD vrátane registrácie doménových mien v rámci TLD a za technickú prevádzku TLD vrátane prevádzky menných serverov, údržby databáz a distribúcie zónových súborov TLD v rámci menných serverov, **pričom sú vylúčené situácie, keď správca používa mená domény najvyššej úrovne výhradne na vlastné účely**;

15a. „subjekty poskytujúce služby registrácie doménových mien pre TLD“ sú správcovia mien TLD, registrátori TLD a agenti registrátorov, ako sú predajcovia a poskytovatelia služieb proxy;

16. „digitálna služba“ je služba v zmysle článku 1 ods. 1 písm. b) smernice Európskeho parlamentu a Rady (EÚ) 2015/1535[35];

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

[35] 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).

16b. „kvalifikovaný poskytovateľ dôveryhodných služieb“ je kvalifikovaný poskytovateľ dôveryhodných služieb v zmysle článku 3 bodu 20 nariadenia (EÚ) č. 910/2014;

17. „online trh“ sú digitálne služby v zmysle článku 2 písm. n) smernice Európskeho parlamentu a Rady 2005/29/ES[36];

18. „internetový vyhľadávač“ je digitálna služba v zmysle článku 2 bodu 5 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/1150[37];

19. „služba cloud computingu“ je digitálna služba, ktorá umožňuje 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;**

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

---

36 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).

37 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).

21. „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;

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

23. „subjekt verejnej správy“ je subjekt, **ktorý je ako taký uznaný v členskom štáte v súlade s vnútroštátnym právom** [...] 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 z väčšej časti financovaný štátnymi, regionálnymi alebo inými verejnoprávnymi inštitúciami; alebo jeho riadenie podlieha dohľadu týchto orgánov alebo inštitúcií; alebo má správnu, riadiacu alebo dozornú radu, v ktorej viac ako polovicu členov menujú štátne, regionálne alebo iné verejnoprávne inštitúcie;

    d) má právomoc vydávať pre fyzické alebo právnické osoby správne alebo regulačné rozhodnutia, ktoré majú vplyv na ich práva pri cezhraničnom pohybe osôb, tovaru, služieb alebo kapitálu.

24. „subjekt“ je každá fyzická alebo právnická osoba zriadená a uznaná za takú podľa vnútroštátneho práva v mieste svojho usadenia, ktorá môže vo vlastnom mene vykonávať práva a podliehať povinnostiam; „kľúčový subjekt“ je subjekt typu označeného ako kľúčový subjekt v prílohe I;

25. „kľúčový subjekt“ je akýkoľvek subjekt typu [...] **ustanoveného v prílohe I, ktorý sa za kľúčový označí v súlade s článkom 2a ods. 1;**

26. „dôležitý subjekt“ je akýkoľvek subjekt typu [...] **ustanoveného v prílohách I a II, ktorý sa za dôležitý označí v súlade s článkom 2a ods. 2;**

26a. „produkt IKT“ je produkt IKT v zmysle článku 2 bodu 12 nariadenia (EÚ) 2019/881;

26aa. „služba IKT“ je služba IKT v zmysle článku 2 bodu 13 nariadenia (EÚ) 2019/881;

26ab. „proces IKT“ je proces IKT v zmysle článku 2 bodu 14 nariadenia (EÚ) 2019/881;

26ac. „poskytovateľ riadených služieb“ je akýkoľvek subjekt, ktorý poskytuje služby, ako sú siete, aplikácie, infraštruktúra a bezpečnosť, prostredníctvom priebežného a pravidelného riadenia, podpory a aktívnej správy v priestoroch zákazníkov, vo svojom dátovom centre (hosting) alebo v dátovom centre tretej strany.

26ad. „poskytovateľ riadených bezpečnostných služieb“ je akýkoľvek subjekt, ktorý vykonáva outsourcing monitorovania a riadenia bezpečnostných zariadení a systémov. Spoločné služby zahŕňajú služby riadeného firewallu, odhaľovania prienikov, virtuálnej súkromnej siete, skenovanie zraniteľnosti a antivírusové služby.

Zahŕňa aj využívanie centier bezpečnostných operácií s vysokou dostupnosťou (buď z vlastných zariadení, alebo z dátových centier iných poskytovateľov) na nepretržité poskytovanie služieb, ktorých cieľom je znížiť počet zamestnancov v oblasti prevádzkovej bezpečnosti, ktorých musí podnik zamestnať, vyškoliť a udržiavať si, aby si zachovával prijateľný stav kybernetickej bezpečnosti.

KAPITOLA II

Koordinované regulačné rámce kybernetickej bezpečnosti

Článok 5

Národná stratégia kybernetickej bezpečnosti

1. Každý členský štát prijme národnú stratégiu kybernetickej bezpečnosti, v ktorej sa vymedzia strategické ciele a vhodné politické a regulačné opatrenia na dosiahnutie a zachovanie vysokej úrovne kybernetickej bezpečnosti. Národná stratégia kybernetickej bezpečnosti sietí obsahuje najmä tieto prvky:

   a) [...] ciele a priority stratégie členských štátov v oblasti kybernetickej bezpečnosti;

   b) riadiaci rámec na dosiahnutie týchto cieľov a priorít vrátane politík uvedených v odseku 2, ako aj úlohy a povinnosti rôznych orgánov a aktérov, ktorí sa podieľajú na vykonávaní stratégie [...];

   c) [...] **usmernenia** s cieľom identifikovať relevantné prostriedky a **posúdiť** riziká v oblasti kybernetickej bezpečnosti v danom členskom štáte [...];

   d) identifikáciu opatrení na zabezpečenie pripravenosti a reakcie na incidenty a obnovy vrátane spolupráce medzi verejným a súkromným sektorom;

   e) [...]

f) politický rámec pre posilnenú koordináciu medzi príslušnými orgánmi podľa tejto smernice a smernice Európskeho parlamentu a Rady (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov][38] na účely výmeny informácií o **kybernetickobezpečnostných rizikách**, [...] kybernetických hrozbách a **incidentoch, ako aj o nekybernetických rizikách, hrozbách a incidentoch** a **prípadne** o vykonávaní úloh dohľadu;

fa) politický rámec pre koordináciu a spoluprácu medzi príslušnými orgánmi podľa tejto smernice a príslušnými orgánmi určenými podľa osobitných právnych predpisov pre jednotlivé odvetvia.

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

a) politiku zameranú na kybernetickú bezpečnosť v dodávateľskom reťazci produktov a služieb IKT, ktoré [...] subjekty používajú na poskytovanie svojich služieb;

b) politiku [...] zahrnutia a špecifikácie požiadaviek týkajúcich sa kybernetickej bezpečnosti produktov a služieb IKT vo verejnom obstarávaní **vrátane certifikácie kybernetickej bezpečnosti**;

c) politiku **riadenia zraniteľností, ktorá zahŕňa podporu a uľahčovanie** [...] **dobrovoľného** koordinovaného zverejňovania informácií o zraniteľnosti v zmysle článku 6 **ods. 1**;

d) politiku súvisiacu s udržaním všeobecnej dostupnosti, [...] integrity a **dôvernosti** verejného jadra otvoreného internetu;

e) politiku podpory a rozvíjania **vzdelávania a odbornej prípravy** a zručností v oblasti kybernetickej bezpečnosti, iniciatívy na zvyšovanie povedomia, ako aj v oblasti výskumu a vývoja;

---

38 *[vložte celý názov a odkaz na uverejnenie v Ú. v., keď budú známe]*

f) politiku podporovania akademických a výskumných inštitúcií pri vývoji nástrojov kybernetickej bezpečnosti a bezpečnej sieťovej infraštruktúry;

g) politiku, príslušné postupy a vhodné nástroje na zdieľanie informácií s cieľom podporovať dobrovoľné zdieľanie informácií o kybernetickej bezpečnosti medzi spoločnosťami v súlade s právom Únie;

h) politiku zameranú na špecifické potreby MSP, najmä tých MSP, ktoré sú vylúčené z rozsahu pôsobnosti tejto smernice, v súvislosti s usmerneniami a podporou pri zlepšovaní ich odolnosti voči kybernetickým [...] hrozbám.

3. Členské štáty oznámia Komisii svoje národné stratégie kybernetickej bezpečnosti do troch mesiacov od ich prijatia. Členské štáty môžu **pritom** vylúčiť **prvky stratégie, ktoré sa týkajú** národnej [...] bezpečnosti.

4. Členské štáty pravidelne a aspoň každých [...] **päť** rokov posudzujú svoje národné stratégie kybernetickej bezpečnosti na základe kľúčových ukazovateľov výkonnosti a v prípade potreby ich menia. Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA) členským štátom na **ich** žiadosť pomáha pri vypracúvaní národnej stratégie a kľúčových ukazovateľov výkonnosti na posúdenie stratégie.

Článok 6

Koordinované zverejňovanie informácií o zraniteľnosti a európsky register zraniteľností

1. Každý členský štát určí jednu zo svojich jednotiek CSIRT v zmysle článku 9 za koordinátora na účely koordinovaného zverejňovania informácií o zraniteľnosti. Určená jednotka CSIRT koná ako dôveryhodný sprostredkovateľ, ktorý v prípade potreby uľahčuje interakciu medzi oznamujúcim subjektom, **osobou zodpovednou za zraniteľnosť** a výrobcom alebo poskytovateľom produktov IKT alebo služieb IKT. **Každá fyzická alebo právnická osoba môže podľa možnosti anonymne nahlásiť zraniteľnosť uvedenú v článku 4 ods. 8 určenej jednotke CSIRT. Určená jednotka CSIRT zabezpečí dôsledné prijatie krokov nadväzujúcich na hlásenie a dôvernosť totožnosti osoby, ktorá zraniteľnosť nahlásila.** Ak by oznámená zraniteľnosť [...] **mohla by mať významný vplyv na subjekty vo viac ako jednom členskom štáte**, určená jednotka CSIRT každého dotknutého členského štátu v **prípade potreby** spolupracuje s **inými určenými jednotkami CSIRT** v rámci siete jednotiek CSIRT.

2. Agentúra ENISA **po konzultácii so skupinou pre spoluprácu** zriadi a udržiava európsky register zraniteľností. Na tento účel agentúra ENISA zriadi a udržiava vhodné informačné systémy, politiky a postupy, najmä s cieľom umožniť dôležitým a kľúčovým subjektom a ich dodávateľom sietí a informačných systémov **dobrovoľne** zverejňovať a registrovať **verejne známe** zraniteľnosti v produktoch IKT alebo službách IKT, ako aj poskytovať prístup k informáciám o zraniteľnosti nachádzajúcich sa v registri všetkým zainteresovaným stranám. Register obsahuje najmä informácie opisujúce zraniteľnosť, zasiahnuté produkty IKT alebo služby IKT a závažnosť zraniteľnosti z hľadiska okolností, za ktorých ju možno zneužiť, dostupnosť súvisiacich bezpečnostných záplat a v prípade, že žiadne nie sú k dispozícii, usmernenie **vydané príslušnými vnútroštátnymi orgánmi alebo jednotkami CSIRT** pre používateľov zraniteľných produktov a služieb o tom, ako možno zmierniť riziká vyplývajúce zo zverejnených zraniteľností. **Agentúra ENISA zabezpečuje, aby európsky register zraniteľností využíval bezpečnú a odolnú komunikačnú a informačnú infraštruktúru.**

Článok 7

Národné rámce krízového riadenia kybernetickej bezpečnosti

1. Každý členský štát určí jeden alebo viac príslušných orgánov zodpovedných za riadenie kybernetickobezpečnostných incidentov a kríz veľkého rozsahu. Členské štáty zabezpečia, aby príslušné orgány mali primerané zdroje na účinné a efektívne vykonávanie zverených úloh. **Členské štáty zabezpečia súlad s existujúcimi rámcami pre všeobecné krízové riadenie.**

2. Každý členský štát určí kapacity, prostriedky a postupy, ktoré možno použiť v prípade krízy na účely tejto smernice.

3. Každý členský štát prijme národný plán reakcie na kybernetickobezpečnostné incidenty a krízy, v ktorom sú stanovené ciele a spôsoby riadenia kybernetickobezpečnostných incidentov a kríz veľkého rozsahu. V pláne sa stanovia najmä tieto prvky:

   a) ciele vnútroštátnych opatrení a činností v oblasti pripravenosti;

   b) úlohy a zodpovednosti vnútroštátnych príslušných orgánov;

   c) postupy krízového riadenia kybernetickej bezpečnosti **vrátane ich začlenenia do všeobecného vnútroštátneho rámca krízového riadenia** a kanálov na výmenu informácií;

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

   e) príslušné verejné a súkromné [...] strany a použitá infraštruktúra;

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

4. Členské štáty [...] **informujú** Komisiu o určení svojich príslušných orgánov uvedených v odseku 1 a predložia **relevantné informácie týkajúce sa požiadaviek odseku 3 tohto článku** o svojich vnútroštátnych plánoch reakcie na kybernetické incidenty a krízy [...] do troch mesiacov od tohto určenia a prijatia uvedených plánov. Členské štáty môžu [...] vylúčiť špecifické informácie, a to v takom prípade a takom rozsahu, v akom je to [...] potrebné pre ich národnú bezpečnosť, **verejnú bezpečnosť alebo obranu.**

Článok 8

Vnútroštátne príslušné orgány a jednotné kontaktné miesta

1. Každý členský štát určí jeden alebo viacero príslušných orgánov zodpovedných za kybernetickú bezpečnosť a za úlohy dohľadu uvedené v kapitole VI tejto smernice. Členské štáty môžu na tento účel určiť už existujúci orgán alebo existujúce orgány.

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

3. Každý členský štát určí jedno vnútroštátne jednotné kontaktné miesto pre kybernetickú bezpečnosť (ďalej len „jednotné kontaktné miesto“). Ak členský štát určí iba jeden príslušný orgán, tento 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 v iných členských štátoch, ako aj zabezpečiť medziodvetvovú spoluprácu s inými príslušnými vnútroštátnymi orgánmi v rámci daného členského štátu.

5. Členské štáty zabezpečia, aby príslušné orgány uvedené v odseku 1 a jednotné kontaktné miesta mali primerané zdroje na účinné a efektívne vykonávanie zverených úloh, a teda na plnenie cieľov tejto smernice. Členské štáty zabezpečia účinnú, efektívnu a bezpečnú spoluprácu určených zástupcov v rámci skupiny pre spoluprácu uvedenej v článku 12.

6. Každý členský štát bez zbytočného odkladu oznámi Komisii určenie príslušného orgánu uvedeného v odseku 1 a jednotného kontaktného miesta uvedeného v odseku 3, ich úlohy a akékoľvek následné zmeny. Každý členský štát svoje určenie uverejní. Komisia uverejní zoznam určených jednotných kontaktných miest.

Článok 9

Jednotky pre riešenie počítačových bezpečnostných incidentov (jednotky CSIRT)

1. Každý členský štát určí jednu alebo viac jednotiek CSIRT, ktoré spĺňajú požiadavky stanovené v článku 10 ods. 1, pokrývajú aspoň odvetvia, pododvetvia alebo subjekty uvedené v prílohách I a II a zodpovedajú za riešenie incidentov podľa presne stanoveného postupu. Jednotku CSIRT možno zriadiť v rámci príslušného orgánu uvedeného v článku 8.

2. Členské štáty zabezpečia, aby každá jednotka CSIRT mala primerané zdroje na účinné plnenie svojich úloh stanovených v článku 10 ods. 2. **Pri vykonávaní týchto úloh môžu jednotky CSIRT uprednostniť poskytovanie konkrétnych služieb subjektom na základe prístupu založeného na riziku.**

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 inými relevantnými zainteresovanými stranami. Členské štáty na tento účel zabezpečia, aby jednotky CSIRT prispievali k zavádzaniu bezpečných nástrojov na výmenu informácií.

4. Jednotky CSIRT spolupracujú a v prípade potreby si vymieňajú relevantné informácie v súlade s článkom 26 s dôveryhodnými odvetvovými alebo medziodvetvovými komunitami kľúčových a dôležitých subjektov.

5. Jednotky CSIRT sa zúčastňujú na partnerskom **zisťovaní**[...] organizovanom v súlade s článkom 16.

6. Členské štáty zabezpečia účinnú, efektívnu a bezpečnú spoluprácu svojich jednotiek CSIRT v rámci siete jednotiek CSIRT uvedenej v článku 13.

7. Členské štáty bez zbytočného odkladu oznámia Komisii jednotky CSIRT určené v súlade s odsekom 1, koordinátora jednotiek CSIRT určeného v súlade s článkom 6 ods. 1 a ich príslušné úlohy stanovené vo vzťahu k subjektom uvedeným v prílohách I a II.

8. Členské štáty môžu pri tvorbe vnútroštátnych jednotiek CSIRT požiadať o pomoc agentúru ENISA.

Článok 10

Požiadavky na jednotky CSIRT a ich úlohy

1. Jednotky CSIRT musia spĺňať tieto požiadavky:

   a) jednotky CSIRT musia zabezpečovať vysokú úroveň dostupnosti svojich komunikačných [...] **kanálov**, a to tak, že predchádzajú tomu, aby zlyhali ako celok, ak zlyhá ich ľubovoľný jediný bod, a musia mať k dispozícii niekoľko spôsobov, ktorými ich možno kedykoľvek kontaktovať a ktorými môžu tieto jednotky kontaktovať iných. Jednotky CSIRT musia jasne špecifikovať komunikačné kanály a oboznámiť s nimi zainteresované strany a spolupracujúcich partnerov;

   b) pracoviská jednotiek CSIRT a podporné informačné systémy musia byť umiestnené na zabezpečených miestach;

c) jednotky CSIRT musia mať zavedený vhodný systém riadenia a zasielania žiadostí, a to najmä s cieľom uľahčiť ich účinné a efektívne odovzdávanie;

d) jednotky CSIRT musia byť primerane personálne vybavené, aby sa zabezpečila stála dostupnosť ich služieb;

e) jednotky CSIRT musia byť vybavené redundantnými systémami a záložným pracovným priestorom na zabezpečenie kontinuity svojich služieb;

f) jednotky CSIRT musia mať možnosť zapojiť sa do sietí medzinárodnej spolupráce.

2. Jednotky CSIRT plnia tieto úlohy:

a) monitorujú kybernetické hrozby, zraniteľnosti a incidenty na vnútroštátnej úrovni;

b) poskytujú kľúčovým a dôležitým subjektom, ako aj **príslušným orgánom a** iným relevantným zainteresovaným stranám včasné varovanie, výstrahy, hlásenia a šíria informácie o kybernetických hrozbách, zraniteľnostiach a incidentoch;

c) reagujú na incidenty;

d) zhromažďujú a analyzujú forenzné údaje a poskytujú dynamickú analýzu rizík a incidentov a situačný prehľad o kybernetickej bezpečnosti;

e) [...] proaktívne kontrolujú siete a informačné systémy [...] s cieľom **odhaľovať zraniteľnosti s potenciálnym závažným vplyvom, a to za predpokladu, že v prípade chýbajúceho súhlasu daného subjektu nedochádza k prienikom do sietí a informačných systémov ani k negatívnemu vplyvu na ich fungovanie;**

f) zapájajú sa do siete jednotiek CSIRT a v **závislosti od svojich kapacít a kompetencií** poskytujú vzájomnú pomoc ostatným členom siete na ich žiadosť;

fa) ak je to uplatniteľné, konajú ako koordinátor na účely postupu koordinovaného zverejňovania informácií o zraniteľnosti podľa článku 6 ods. 1, čo zahŕňa najmä uľahčovanie interakcie medzi oznamujúcimi subjektmi, osobou zodpovednou za zraniteľnosť a výrobcom alebo poskytovateľom produktov IKT alebo služieb IKT v prípadoch, keď je to potrebné, identifikovanie a kontaktovanie dotknutých subjektov, podporovanie oznamujúcich subjektov, dojednanie harmonogramov zverejňovania informácií a riadenie zraniteľností, ktoré majú vplyv na viaceré organizácie (viacstranné koordinované zverejňovanie informácií o zraniteľnosti).

3. Jednotky CSIRT nadviažu spoluprácu s príslušnými aktérmi v súkromnom sektore s cieľom lepšie dosiahnuť ciele smernice.

3a. Jednotky CSIRT môžu nadviazať vzťahy spolupráce s vnútroštátnymi jednotkami CSIRT tretích krajín. V rámci tejto spolupráce si môžu vymieňať relevantné informácie vrátane osobných údajov v súlade s právom Únie týkajúcim sa ochrany údajov.

4. Jednotky CSIRT v záujme uľahčenia spolupráce podporujú prijímanie a využívanie spoločných alebo normalizovaných postupov, režimov utajenia a taxonómie v súvislosti s týmito prvkami:

a) postupy riešenia incidentov;

b) krízové riadenie kybernetickej bezpečnosti;

c) koordinované zverejňovanie informácií o zraniteľnosti.

Článok 11

Spolupráca na vnútroštátnej úrovni

1. Ak príslušné orgány uvedené v článku 8, jednotné kontaktné miesto a jednotky CSIRT jedného členského štátu sú samostatnými subjektmi, pri plnení povinností stanovených v tejto smernici vzájomne spolupracujú.

2. Členské štáty zabezpečia, aby ich príslušné orgány alebo jednotky CSIRT dostávali oznámenia o incidentoch, významných kybernetických hrozbách a udalostiach odvrátených v poslednej chvíli predkladané podľa tejto smernice. Ak členský štát rozhodne, že jeho jednotky CSIRT nemajú dostávať tieto oznámenia, jednotkám CSIRT sa v rozsahu potrebnom na plnenie ich úloh poskytne prístup k údajom o incidentoch, ktoré oznámili kľúčové alebo dôležité subjekty podľa článku 20.

3. Členské štáty zabezpečia, aby ich príslušné orgány alebo jednotky CSIRT informovali jednotné kontaktné miesto o oznámeniach o incidentoch, významných kybernetických hrozbách a udalostiach odvrátených v poslednej chvíli predkladaných podľa tejto smernice.

4. Členské štáty v rozsahu potrebnom na účinné plnenie úloh a povinností stanovených v tejto smernici zabezpečia v rámci daného členského štátu primeranú spoluprácu medzi príslušnými orgánmi, **jednotkami CSIRT,** jednotnými kontaktnými miestami, a ako aj orgánmi presadzovania práva, orgánmi na ochranu údajov a **príslušnými** orgánmi **určenými** [...] podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov], **príslušnými orgánmi podľa vykonávacieho nariadenia Komisie 2019/1583, vnútroštátnymi regulačnými orgánmi určenými v súlade so smernicou (EÚ) 2018/1972, vnútroštátnymi orgánmi určenými v súlade s článkom 17 nariadenia (EÚ) č. 910/2014,** [...] vnútroštátnymi finančnými orgánmi určenými v súlade s nariadením Európskeho parlamentu a Rady (EÚ) XXXX/XXXX [nariadenie DORA]**, ako aj príslušnými orgánmi určenými na základe iných právnych aktov Únie platných pre jednotlivé odvetvia**.

5. Členské štáty zabezpečia, aby si ich príslušné orgány **podľa tejto smernice a príslušné orgány určené podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov]** pravidelne **vymieňali** [...] informácie [...] o **identifikácii kritických subjektov,** kybernetickobezpečnostných rizikách, kybernetických **hrozbách a incidentoch, ako aj o iných ako kybernetických rizikách, hrozbách a incidentoch**, ktoré zasiahli kľúčové subjekty identifikované ako kritické **[**alebo rovnocenné s kritickými subjektmi**]** podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov], ako aj o opatreniach prijatých [...] v reakcii na tieto riziká a incidenty. **Členské štáty tiež zabezpečia, aby si príslušné orgány podľa tejto smernice** [...] **a príslušné orgány určené podľa nariadenia XXXX/XXXX [nariadenie DORA], smernice 2018/1972 a nariadenia (EÚ) 910/2014 pravidelne vymieňali relevantné informácie**.

Pokiaľ ide o poskytovateľov dôveryhodných služieb a [...] najmä[...] v prípadoch, keď je úloha dohľadu podľa tejto smernice pridelená inému orgánu ako orgánom dohľadu určeným podľa nariadenia (EÚ) 910/2014, vnútroštátne orgány podľa tejto smernice úzko a včas spolupracujú formou výmeny relevantných informácií s cieľom zabezpečiť účinný dohľad a súlad poskytovateľov dôveryhodných služieb s požiadavkami stanovenými v tejto smernici a nariadení [XXXX/XXXX]**, pričom v prípade potreby vnútroštátny príslušný orgán v zmysle tejto smernice bez zbytočného odkladu informuje orgán dohľadu eIDAS o každej oznámenej významnej kybernetickej hrozbe alebo incidente s dosahom na dôveryhodné služby**.

5a. Na účely[...] zjednodušenia oznamovania incidentov môžu členské štáty zriadiť jednotný vstupný bod pre všetky oznámenia požadované podľa tejto smernice, ako aj podľa nariadenia (EÚ) 2016/679 a smernice 2002/58/ES. Členské štáty môžu používať jednotný vstupný bod na oznámenia požadované podľa právnych aktov Únie platných pre jednotlivé odvetvia. Jednotný vstupný bod nemá vplyv na uplatňovanie ustanovení nariadenia (EÚ) 2016/679 a smernice 2002/58/ES, najmä tých, ktoré sa týkajú nezávislých dozorných orgánov.

KAPITOLA III

*Spolupráca v **rámci EÚ***

Článok 12

Skupina pre spoluprácu

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

2. Skupina pre spoluprácu si plní úlohy na základe dvojročných pracovných programov uvedených v odseku 6.

3. Skupina pre spoluprácu sa skladá zo zástupcov členských štátov, Komisie a agentúry ENISA. Na činnostiach skupiny pre spoluprácu sa ako pozorovateľ zúčastňuje Európska služba pre vonkajšiu činnosť. Na činnostiach skupiny pre spoluprácu sa v **súlade s článkom 42 ods. 1 nariadenia (EÚ) XXXX/XXXX [nariadenie DORA]** [...] môžu zúčastňovať európske orgány dohľadu (ESA) a **príslušné orgány určené podľa nariadenia (EÚ) XXXX/XXXX [nariadenie DORA]**.

   Vo vhodných prípadoch môže skupina pre spoluprácu prizvať k svojej práci zástupcov príslušných zainteresovaných strán.

   Sekretariát zabezpečuje Komisia.

4. Skupina pre spoluprácu plní tieto úlohy:

   a) poskytovanie usmernení príslušným orgánom v súvislosti s transpozíciou a vykonávaním tejto smernice**;**

   aa) poskytovanie usmernení v súvislosti s vypracúvaním a vykonávaním politík týkajúcich sa koordinovaného zverejňovania informácií o zraniteľnosti, ako sa uvádza v článku 5 ods. 2 písm. c) a v článku 6 ods. 1;

   b) výmena najlepších postupov a informácií v súvislosti s vykonávaním tejto smernice, a to aj pokiaľ ide o kybernetické hrozby, incidenty, zraniteľnosti, udalosti odvrátené

v poslednej chvíli, iniciatívy na zvyšovanie povedomia, odbornú prípravu, cvičenia a zručnosti, budovanie kapacít, ako aj normy a technické špecifikácie;

c) vzájomné poradenstvo a spolupráca s Komisiou v súvislosti s novými politickými iniciatívami v oblasti kybernetickej bezpečnosti;

d) vzájomné poradenstvo a spolupráca s Komisiou v súvislosti s návrhom vykonávacích [...] aktov Komisie prijatých podľa tejto smernice;

e) výmena najlepších postupov a informácií s príslušnými inštitúciami, orgánmi, úradmi a agentúrami Únie;

ea) výmena názorov na vykonávanie odvetvových právnych predpisov vyznačujúcich sa aspektami kybernetickej bezpečnosti;

f) prediskutovanie správ o partnerskom [...] **zisťovaní**, ako sa uvádza v článku 16 ods. 7;

g) prediskutovanie **skúseností** [...] **zo** spoločných činností dohľadu v cezhraničných prípadoch, ako sa uvádza v článku 34;

h) poskytovanie strategických usmernení sieti jednotiek CSIRT **a sieti EU–CyCLONe** v súvislosti s konkrétnymi vznikajúcimi otázkami;

ha) výmena názorov na politické opatrenia nadväzujúce na rozsiahle kybernetickobezpečnostné incidenty, a to na základe skúseností získaných zo siete jednotiek CSIRT a siete EU–CyCLONe;

i) prispievanie ku kybernetickobezpečnostným schopnostiam v celej Únii uľahčovaním výmeny vnútroštátnych úradníkov prostredníctvom programu budovania kapacít, do ktorého sú zapojení zamestnanci z príslušných orgánov členských štátov alebo jednotiek CSIRT;

j) organizovanie pravidelných spoločných stretnutí s príslušnými súkromnými zainteresovanými stranami z celej Únie s cieľom prediskutovať činnosti skupiny a zhromažďovať informácie o nových politických výzvach;

k) prediskutovanie práce vykonanej v súvislosti s kybernetickobezpečnostnými cvičeniami vrátane práce agentúry ENISA**;**

ka) vytvorenie mechanizmu partnerského zisťovania v súlade s článkom 16 tejto smernice.

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

6. Do ... [24 mesiacov po nadobudnutí účinnosti tejto smernice] a potom každé dva roky skupina pre spoluprácu zostavuje pracovný program týkajúci sa činností, ktoré sa majú vykonávať v rámci plnenia jej cieľov a úloh. Časový rámec prvého programu prijatého podľa tejto smernice sa zosúladí s časovým rámcom posledného programu prijatého podľa smernice (EÚ) 2016/1148.

7. Komisia môže prijať vykonávacie akty stanovujúce procesné opatrenia potrebné na fungovanie skupiny pre spoluprácu. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania, na ktorý sa odkazuje v článku 37 ods. 2.

8. Skupina pre spoluprácu sa pravidelne a aspoň raz ročne stretáva so skupinou pre odolnosť kritických subjektov zriadenou podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov] s cieľom podporovať strategickú spoluprácu a **uľahčovať** výmenu informácií.

Článok 13

Sieť jednotiek CSIRT

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

2. Sieť jednotiek CSIRT sa skladá zo zástupcov jednotiek CSIRT členských štátov **určených v súlade s článkom 9** a jednotky CERT-EU. Komisia sa zúčastňuje na práci siete jednotiek CSIRT ako pozorovateľ. Agentúra ENISA zabezpečuje sekretariát a aktívne podporuje spoluprácu medzi jednotkami CSIRT.

3. Sieť jednotiek CSIRT plní tieto úlohy:

   a) výmena informácií o schopnostiach jednotiek CSIRT;

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

ba) výmena informácií v súvislosti s publikáciami a odporúčaniami týkajúcimi sa kybernetickej bezpečnosti;

bb) zdieľanie technických riešení uľahčujúcich technické riešenie incidentov;

bc) výmena najlepších postupov, nástrojov a procesov v súvislosti s úlohami jednotiek CSIRT;

c) na žiadosť [...] **člena** siete jednotiek CSIRT potenciálne zasiahnutého incidentom výmena a prediskutovanie informácií o danom incidente a súvisiacich kybernetických hrozbách, rizikách a zraniteľnostiach;

d) na žiadosť [...] **člena** siete jednotiek CSIRT prediskutovanie a pokiaľ možno vykonanie koordinovanej reakcie na incident, ktorý bol identifikovaný v jurisdikcii daného členského štátu;

e) poskytovanie podpory členským štátom pri riešení cezhraničných incidentov podľa tejto smernice;

f) spolupráca**, výmena najlepších postupov** a poskytovanie pomoci určeným jednotkám CSIRT uvedeným v článku 6, pokiaľ ide o riadenie [...] koordinovaného zverejňovania informácií o zraniteľnostiach, ktoré zasiahli viacerých výrobcov alebo poskytovateľov produktov IKT, služieb IKT a procesov IKT, ktorí majú sídlo v rôznych členských štátoch;

g) 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 spôsobmi koordinácie pri reakcii na cezhraničné riziká a incidenty;

v) s príspevkom na **žiadosť členského štátu** k národnému plánu reakcie na kybernetickobezpečnostné incidenty a krízy uvedeného v článku 7 ods. 3;

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

i) bilancia kybernetickobezpečnostných cvičení vrátane cvičení organizovaných agentúrou ENISA;

j) na žiadosť niektorej jednotky CSIRT prediskutovanie schopností a pripravenosti tejto jednotky CSIRT;

k) spolupráca a výmena informácií s regionálnymi a únijnými centrami bezpečnostných operácií (SOC) s cieľom zlepšiť spoločný situačný prehľad o incidentoch a hrozbách v celej Únii;

l) prediskutovanie správ o partnerskom [...] **zisťovaní** uvedených v článku 16 ods. 7;

m) vydávanie 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 35 sieť jednotiek CSIRT do [24 mesiacov odo dňa nadobudnutia účinnosti tejto smernice] a potom každé dva roky posúdi pokrok dosiahnutý v rámci operačnej spolupráce a vypracuje správu. V správe sa predovšetkým vyvodia závery o výsledkoch partnerského [...] **zisťovania** uvedeného v článku 16 a vykonaného v súvislosti s vnútroštátnymi jednotkami CSIRT vrátane záverov a odporúčaní, ktoré sa vykonávajú podľa tohto článku. Táto správa sa tiež predloží skupine pre spoluprácu.

5. Sieť jednotiek CSIRT prijme vlastný rokovací poriadok.

6. Sieť EU-CyCLONe spolupracuje so sieťou jednotiek CSIRT na základe dohodnutých procedurálnych dojednaní.

Článok 14

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

1. S cieľom podporiť koordinované riadenie rozsiahlych kybernetickobezpečnostných incidentov a kríz na operačnej úrovni a zabezpečiť pravidelnú výmenu informácií medzi členskými štátmi a inštitúciami, orgánmi a agentúrami Únie sa týmto zriaďuje Európska sieť styčných organizácií pre kybernetické krízy (EU-CyCLONe).

2. Sieť EU-CyCLONe tvoria zástupcovia orgánov **kybernetického** krízového riadenia členských štátov určených v súlade s článkom 7 [...]. **Komisia sa zúčastňuje na činnosti siete ako pozorovateľ.** Agentúra ENISA zabezpečuje sekretariát siete, podporuje bezpečnú výmenu informácií a **poskytuje potrebné nástroje na podporu spolupráce medzi členskými štátmi zabezpečujúcimi bezpečnú výmenu informácií.**

Vo vhodných prípadoch môže sieť EU-CyCLONe prizvať k svojej práci zástupcov príslušných zainteresovaných strán.

3. Sieť EU-CyCLONe plní tieto úlohy:

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

b) vytváranie spoločného situačného prehľadu o [...] rozsiahlych kybernetickobezpečnostných incidentoch a krízach;

ba) posudzovanie dôsledkov a vplyvu relevantných rozsiahlych kybernetickobezpečnostných incidentov a navrhovanie možných zmierňujúcich opatrení;

c) koordinácia **riadenia** rozsiahlych kybernetickobezpečnostných incidentov a kríz [...], ako aj podpora rozhodovania na politickej úrovni v súvislosti s takýmito incidentmi a krízami;

d) **na žiadosť členského štátu** prediskutovanie **jeho** národných plánov reakcie na kybernetickobezpečnostné incidenty a **krízy** uvedených v článku 7 ods. **3[...];**[...]

4. Sieť EU-CyCLONe prijme svoj rokovací poriadok.

5. Sieť EU-CyCLONe pravidelne podáva skupine pre spoluprácu správy o **riadení rozsiahlych kybernetickobezpečnostných incidentov a kríz** [...], pričom sa zameriava najmä na ich vplyv na kľúčové a dôležité subjekty.

6. Sieť EU-CyCLONe spolupracuje so sieťou jednotiek CSIRT na základe dohodnutých procedurálnych opatrení.

7. Sieť EU-CyCLONe predloží Európskemu parlamentu a Rade správu hodnotiacu jej činnosť do [24 mesiacov po nadobudnutí účinnosti tejto smernice].

Článok 14a

Medzinárodná spolupráca

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

Článok 15

Správa o stave kybernetickej bezpečnosti v Únii

1. Agentúra ENISA v spolupráci s Komisiou a **skupinou pre spoluprácu** vydáva každé dva roky správu o stave kybernetickej bezpečnosti v Únii. Správa obsahuje **najmä** [...]:

   aa) posúdenie kybernetickobezpečnostného rizika na úrovne Únie s prihliadnutím na rozmanitosť hrozieb;

   a) [...] **posúdenie** rozvoja kybernetickobezpečnostných schopností vo verejnom a súkromnom sektore v celej Únii;

   b) [...]

   c) **súhrnné posúdenie na základe kvantitatívnych a kvalitatívnych ukazovateľov týkajúcich sa** kybernetickej bezpečnosti [...], ktoré poskytne **prehľad** o úrovni vyspelosti kybernetickobezpečnostných schopností **vrátane schopností jednotlivých odvetví**.

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

Článok 16

Partnerské zisťovania

1. **S cieľom posilniť vzájomnú dôveru, dosiahnuť vysokú spoločnú úroveň kybernetickej bezpečnosti, ako aj posilniť schopnosti a politiky členských štátov v oblasti kybernetickej bezpečnosti potrebné na účinné vykonávanie tejto smernice skupina** [...] **pre spoluprácu s podporou Komisie** a po konzultácii [...] s agentúrou ENISA**, a prípadne sieťou jednotiek CSIRT** najneskôr **24 [...]** mesiacov od nadobudnutia účinnosti tejto smernice stanoví metodiku [...] **pre objektívny, nediskriminačný a spravodlivý** systém partnerského [...] **zisťovania týkajúci sa** [...] **vykonávania tejto smernice** zo strany členských štátov. **Účasť na partnerskom zisťovaní je dobrovoľná.** Tento **systém pozostáva z hodnotiacich kôl** [...], ktoré vedú experti na kybernetickú bezpečnosť z členských štátov [...] a zahŕňa **jeden alebo viacero** týchto aspektov:

   i) [...] vykonávanie požiadaviek, ktoré sa týkajú riadenia kybernetickobezpečnostných rizík, a oznamovacích povinností uvedených v článkoch 18 a 20;

   ii) [...] schopnosti, vrátane dostupných [...] zdrojov, a [...] plnenie úloh vnútroštátnych príslušných orgánov **uvedených v článku 8 a jednotiek CSIRT uvedených v článku 9**;

[...]

ii**i**) [...] **vykonávanie** vzájomnej pomoci uvedenej v článku 34;

iv) [...] **vykonávanie** rámca na zdieľanie informácií uvedeného v článku 26 tejto smernice [...].

2. **Kritériá, na základe ktorých majú členské štáty určiť expertov oprávnených zúčastniť sa na kolách partnerského zisťovania, sú** [...] objektívne, nediskriminačné, spravodlivé a transparentné [...] a **sú zahrnuté do metodiky uvedenej v odseku 1**. Agentúra ENISA a Komisia [...] **môžu** určiť expertov, ktorí sa ako pozorovatelia zúčastňujú na **kolách partnerského zisťovania**. [...]

3. [...] .

3a. Členské štáty môžu pred začatím kôl partnerského zisťovania vykonať sebahodnotenie aspektov, na ktoré sa dané kolo partnerského zisťovania zameriava, a poskytnúť toto sebahodnotenie určeným expertom uvedeným v odseku 2.

4. Partnerské [...] **zisťovania môžu** zahŕňať [...] **fyzické** alebo virtuálne návštevy na mieste a výmenu informácií na diaľku. So zreteľom na zásadu dobrej spolupráce poskytnú členské štáty, **ktoré sa zúčastňujú na partnerskom zisťovaní**, určeným expertom [...] informácie potrebné na hodnotenie [...]**, bez toho, aby boli dotknuté vnútroštátne alebo únijné právne predpisy týkajúce sa ochrany dôverných alebo utajovaných skutočností alebo ochrany základných funkcií štátu, ako je národná bezpečnosť**. Všetky informácie získané v procese partnerského [...] **zisťovania** sa použijú výlučne na uvedený účel. Experti, ktorí sa zúčastňujú na partnerskom [...] **zisťovaní**, nesmú sprístupniť tretím stranám žiadne citlivé alebo dôverné informácie získané v [...] **tejto súvislosti**. **Členský štát, ktorý sa zúčastňuje na partnerskom zisťovaní, môže na základe riadne opodstatnených dôvodov oznámených skupine pre spoluprácu namietať proti určeniu konkrétnych expertov.**

5. Tie isté aspekty po [...] **tom, ako boli predmetom kola partnerského zisťovania,** nie sú predmetom ďalších **kôl** partnerského [...] **zisťovania pre zúčastnené** členské **štáty** počas [...] **štyroch** rokov od ukončenia **tohto** [...] **kola** partnerského **zisťovania, pokiaľ o to nepožiada dotknutý členský štát alebo s tým na základe návrhu** [...] **skupiny pre spoluprácu nesúhlasí[...]**.

6. [...]

7. Experti zúčastňujúci sa na **kolách** partnerských [...] **zisťovaní** vypracujú návrhy správ o zisteniach a záveroch [...] **hodnotení**. **Členským štátom sa umožní poskytnúť vyjadrenie k ich príslušným návrhom správ, ktoré sa pripojí k správe. Záverečné** správy sa predložia skupine pre spoluprácu[...] **Členské štáty môžu rozhodnúť, že svoje príslušné správy sprístupnia verejnosti.**

KAPITOLA IV

Povinnosti týkajúce sa riadenia kybernetickobezpečnostných rizík a oznamovania

ODDIEL I

Riadenie kybernetickobezpečnostných rizík a oznamovanie

Článok 17

Riadenie

1. Členské štáty zabezpečia, aby riadiace orgány kľúčových a dôležitých subjektov schválili opatrenia na riadenie kybernetickobezpečnostných rizík, ktoré tieto subjekty prijali s cieľom dosiahnuť súlad s článkom 18, [...] **aby** dohliadali na jeho vykonávanie a [...] aby sa od nich **mohla vyžadovať** zodpovednosť za to, ak subjekty nedodržiavajú povinnosti podľa tohto článku.

   Uplatňovaním tohto odseku nie sú dotknuté vnútroštátne právne predpisy členského štátu, pokiaľ ide o pravidlá zodpovednosti vo verejných inštitúciách, ako aj zodpovednosť štátnych zamestnancov a volených a vymenovaných úradníkov.

2. Členské štáty zabezpečia, aby **členovia riadiaceho orgánu** [...] **mali povinnosť** pravidelne absolvovať [...] odbornú prípravu s cieľom získať dostatočné znalosti a zručnosti s cieľom zachytiť a posúdiť riziká a postupy riadenia v oblasti kybernetickej bezpečnosti a ich vplyv na činnosť subjektu.

Článok 18

Opatrenia na riadenie kybernetickobezpečnostných rizík

1**a. Touto smernicou sa uplatňuje prístup „všetkých nebezpečenstiev“, ktorý zahŕňa ochranu sietí a informačných systémov a ich fyzického prostredia pred akoukoľvek udalosťou, ktorá by mohla ohroziť dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov.**

1. Členské štáty zabezpečia, aby kľúčové a dôležité subjekty prijali vhodné a primerané technické a organizačné opatrenia na riadenie rizík súvisiacich s bezpečnosťou sietí a informačných systémov, ktoré tieto subjekty využívajú pri poskytovaní svojich služieb. S ohľadom na najnovší technický vývoj a **náklady na vykonávanie** tieto opatrenia zabezpečujú takú úroveň bezpečnosti sietí a informačných systémov, ktorá zodpovedá miere daného rizika. **Pri posudzovaní primeranosti týchto opatrení sa náležite zohľadní stupeň vystavenia subjektu rizikám, jeho veľkosť, pravdepodobnosť výskytu incidentov a ich závažnosť. Vzhľadom na úroveň a druh rizika pre spoločnosť v prípade incidentov ovplyvňujúcich kľúčové alebo dôležité subjekty môžu byť opatrenia na riadenie kybernetickobezpečnostných rizík uložené dôležitému subjektu menej prísne ako opatrenia uložené kľúčovému subjektu.**

2. Opatrenia uvedené v odseku 1 obsahujú aspoň:

a) analýzu rizika a bezpečnostné politiky informačného systému;

b) riešenie incidentov (predchádzanie incidentom, ich odhaľovanie, [...] reakcia na ne a **obnova po** [...] nich);

c) kontinuita činností a krízové riadenie;

d) bezpečnosť dodávateľského reťazca vrátane bezpečnostných aspektov týkajúcich sa vzťahov medzi každým subjektom a jeho **priamymi** dodávateľmi alebo poskytovateľmi služieb, ako sú napríklad poskytovatelia služieb ukladania a spracúvania dát alebo riadených bezpečnostných služieb;

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

f) politiky a postupy [...] na posúdenie účinnosti opatrení na riadenie kybernetickobezpečnostných rizík;

g) **postupy** týkajúce sa používania kryptografie a šifrovania;

ga) bezpečnosť ľudských zdrojov, zásady kontroly prístupu a správu aktív.

3. Členské štáty zabezpečia, aby subjekty pri zvažovaní vhodných opatrení uvedených v odseku 2 písm. d) [...] **mali povinnosť** zohľadniť zraniteľnosti špecifické pre každého **priameho** dodávateľa a poskytovateľa služieb a celkovú kvalitu produktov a prax ich dodávateľov a poskytovateľov služieb v oblasti kybernetickej bezpečnosti vrátane ich postupov bezpečného vývoja. **Členské štáty tiež zabezpečia, aby subjekty pri zvažovaní vhodných opatrení uvedených v odseku 2 písm. d) mali povinnosť zohľadniť výsledky koordinovaných posúdení rizík vykonaných v súlade s článkom 19 ods. 1.**

4. Členské štáty zabezpečia, aby subjekt po zistení, že jeho služby alebo úlohy nie sú v súlade s požiadavkami stanovenými v odseku 2, prijal bez zbytočného odkladu všetky potrebné nápravné opatrenia a danú službu s týmito požiadavkami zosúladil.

5. Komisia môže prijať vykonávacie akty s cieľom stanoviť technické a metodické špecifikácie prvkov uvedených v odseku 2 **tohto článku, a v prípade potreby aj odvetvové špecifikácie týchto prvkov**. **Komisia prijme do [18 mesiacov od nadobudnutia účinnosti tejto smernice] vykonávacie akty s cieľom stanoviť technické a metodické špecifikácie pre subjekty uvedené v článku 24 ods. 1 a poskytovateľov dôveryhodných služieb uvedených v bode 8 prílohy I. Tieto vykonávacie akty sa prijmú v súlade s postupom preskúmania, na ktorý sa odkazuje v článku 37 ods. 2.** Pri [...] vypracúvaní [...] **týchto vykonávacích** aktov Komisia [...] v čo najväčšej miere **dodržiava** medzinárodné a európske normy, ako aj príslušné technické špecifikácie a **v súvislosti s návrhom vykonávacieho aktu sa radí so skupinou pre spoluprácu a s agentúrou ENISA v súlade s článkom 12 ods. 4 písm. d).**

6. [...]

Článok 19

Koordinované posúdenia rizika kritických dodávateľských reťazcov na úrovni EÚ

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

2. Komisia po konzultácii so skupinou pre spoluprácu a agentúrou ENISA určí konkrétne kritické služby, systémy alebo produkty IKT, ktoré môžu podliehať koordinovanému posúdeniu rizika uvedenému v odseku 1.

Článok 20

Oznamovacie povinnosti

1. Členské štáty zabezpečia, aby kľúčové a dôležité subjekty bez zbytočného odkladu oznámili príslušným orgánom alebo jednotke CSIRT v súlade s odsekmi 3 a 4 každý incident so závažným vplyvom na poskytovanie ich služieb. V prípade potreby tieto subjekty bez zbytočného odkladu oznámia príjemcom svojich služieb **tie** incidenty, ktoré by mohli nepriaznivo ovplyvniť poskytovanie daných služieb. Členské štáty zabezpečia, aby tieto subjekty oznamovali okrem iného informácie umožňujúce príslušným orgánom alebo jednotke CSIRT určiť prípadný cezhraničný vplyv incidentu. **Samotným vykonaním oznámenia sa oznamujúcemu subjektu neukladá väčšia zodpovednosť.**

2. [...]

[...] **Kľúčové a dôležité** subjekty v príslušných prípadoch bez zbytočného odkladu oznámia príjemcom svojich služieb, ktorých potenciálne zasiahla závažná kybernetická hrozba, všetky opatrenia alebo nápravné kroky, ktoré títo príjemcovia môžu v reakcii na danú hrozbu prijať. Subjekty v prípade potreby týmto príjemcom oznámia aj informáciu o samotnej hrozbe. Samotným vykonaním oznámenia sa oznamujúcemu subjektu neukladá väčšia zodpovednosť.

3. Incident sa považuje za závažný, ak:

a) dotknutému subjektu spôsobil alebo môže spôsobiť **vážne** [...] prevádzkové narušenie **služby** alebo finančné straty;

b) zasiahol alebo môže zasiahnuť iné fyzické alebo právnické osoby spôsobením značných hmotných alebo nehmotných strát.

4. Členské štáty zabezpečia, aby dotknuté subjekty na účely oznámenia podľa odseku 1 predložili príslušným orgánom alebo jednotke CSIRT:

a) bez zbytočného odkladu a v každom prípade do 24 hodín od zistenia incidentu prvotné oznámenie, **ktoré sa považuje za včasné varovanie** a v ktorom sa prípadne uvedie, či incident pravdepodobne spôsobilo nezákonné alebo zlomyseľné konanie;

b) na žiadosť príslušného orgánu alebo jednotky CSIRT priebežnú správu o relevantných aktualizáciách daného stavu;

c) najneskôr jeden mesiac po predložení [...] **prvotného oznámenia** podľa písmena a) **záverečnú** správu, ktorá obsahuje aspoň tieto informácie:

i) podrobný opis incidentu, jeho závažnosť a vplyv;

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

iii) uplatnené a prebiehajúce zmierňujúce opatrenia.

Členské štáty zabezpečia, aby sa v riadne odôvodnených prípadoch a po dohode s príslušnými orgánmi alebo jednotkou CSIRT mohol príslušný subjekt odchýliť od lehôt stanovených v písmenách a) a c). **Odchýlku od lehoty uvedenej v písmene c) možno odôvodniť najmä v prípadoch, keď incident stále prebieha.**

5. Príslušné vnútroštátne orgány alebo jednotka CSIRT poskytnú oznamujúcemu subjektu [...] **bez zbytočného odkladu** od prijatia prvotného oznámenia uvedeného v odseku 4 písm. a) odpoveď vrátane počiatočnej spätnej väzby k incidentu a na žiadosť subjektu usmernenia k vykonávaniu možných zmierňujúcich opatrení. Ak jednotka CSIRT nedostala oznámenie uvedené v odseku 1, usmernenie poskytne príslušný orgán v spolupráci s jednotkou CSIRT. Jednotka CSIRT poskytne doplňujúcu technickú podporu, ak o to príslušný subjekt požiada. Ak existuje podozrenie, že incident má trestnoprávnu povahu, príslušné vnútroštátne orgány alebo jednotka CSIRT poskytnú aj usmernenia týkajúce sa oznamovania incidentu orgánom presadzovania práva.

6. V prípade potreby, a najmä ak sa incident uvedený v odseku 1 týka dvoch alebo viacerých členských štátov, príslušný orgán, jednotka CSIRT alebo **jednotné kontaktné miesto** informuje o incidente ostatné zasiahnuté členské štáty a agentúru ENISA. **Dané informácie obsahujú aspoň prvky stanovené v odseku 4 tohto článku.** Príslušné orgány, jednotky CSIRT a jednotné kontaktné miesta pri tom v súlade s právom Únie alebo vnútroštátnymi právnymi predpismi, ktoré sú v súlade s právom Únie, chránia bezpečnosť a obchodné záujmy subjektu, ako aj dôvernosť poskytnutých informácií.

7. Po porade s dotknutým subjektom môže príslušný orgán alebo jednotka CSIRT a prípadne orgány alebo jednotky CSIRT ďalších dotknutých členských štátov informovať o incidente verejnosť alebo požiadať o to daný subjekt, ak je informovanosť verejnosti potrebná na zabránenie incidentu alebo riešenie prebiehajúceho incidentu alebo ak je zverejnenie incidentu vo verejnom záujme z iného dôvodu.

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

9. Jednotné kontaktné miesto predkladá agentúre ENISA [...] **každých šesť mesiacov** súhrnnú správu s anonymizovanými a agregovanými údajmi o incidentoch, závažných kybernetických hrozbách a udalostiach odvrátených v poslednej chvíli oznámených v súlade s odsekom[...] 1 [...] a v súlade s článkom 27. S cieľom prispieť k poskytovaniu porovnateľných informácií môže agentúra ENISA vydať technické usmernenia týkajúce sa parametrov informácií uvedených v súhrnnej správe. **Agentúra ENISA každých šesť mesiacov informuje skupinu pre spoluprácu a sieť jednotiek CSIRT o svojich zisteniach týkajúcich sa doručených oznámení.**

10. Príslušné orgány poskytnú príslušným orgánom určeným podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov] informácie o incidentoch a kybernetických hrozbách, ktoré v súlade s odsekmi 1 a 2 oznámili kľúčové subjekty identifikované ako kritické subjekty alebo ako subjekty rovnocenné s kritickými subjektmi podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov].

11. Komisia môže prijať vykonávacie akty, v ktorých bližšie určí druh informácií, formát a postup oznámenia predkladaného podľa odsekov 1 a 2. Komisia môže prijať aj vykonávacie akty s cieľom ďalej konkretizovať prípady, v ktorých sa incident považuje za závažný, ako sa uvádza v odseku 3. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania, na ktorý sa odkazuje v článku 37 ods. 2.

Článok 21

Použitie európskych systémov certifikácie kybernetickej bezpečnosti

1. S cieľom preukázať súlad s určitými požiadavkami článku 18 môžu **členské štáty vyžadovať, aby subjekty používali konkrétne produkty** [...]**, služby** [...] a **procesy IKT certifikované** v rámci osobitných európskych systémov certifikácie kybernetickej bezpečnosti prijatých podľa článku 49 nariadenia (EÚ) 2019/881. Produkty, služby a procesy **IKT**, ktoré podliehajú certifikácii, môže vytvoriť kľúčový alebo dôležitý subjekt alebo sa môžu obstarať od tretích strán.

2. Komisia môže [...] prijať [...] **vykonávacie** akty, v ktorých bližšie určí, od ktorých kategórií kľúčových **alebo dôležitých** subjektov sa vyžaduje **používanie určitých certifikovaných produktov, služieb a procesov IKT alebo** získanie certifikátu [...] v rámci ktorých [...] európskych systémov certifikácie kybernetickej bezpečnosti **prijatých podľa článku 49 nariadenia (EÚ) 2019/881. Tieto vykonávacie akty sa prijmú v súlade s postupom preskúmania, na ktorý sa odkazuje v článku 37 ods. 2. Pri príprave takýchto vykonávacích aktov Komisia v súlade s článkom 56 nariadenia (EÚ) 2019/881:**

   i) zohľadní vplyv opatrení na výrobcov alebo poskytovateľov takýchto produktov, služieb alebo procesov IKT a na používateľov z hľadiska nákladov na uvedené opatrenia a spoločenských alebo ekonomických prínosov vyplývajúcich z predpokladanej zvýšenej úrovne bezpečnosti cielených produktov, služieb alebo procesov IKT, ako aj ich alternatívnej dostupnosti na trhu;

   ii) vykoná otvorené, transparentné a inkluzívne konzultácie so všetkými príslušnými zainteresovanými stranami a členskými štátmi;

iii) zohľadní všetky lehoty na vykonávanie, prechodné opatrenia a obdobia, najmä s ohľadom na možný vplyv daných opatrení na výrobcov alebo poskytovateľov produktov, služieb a procesov IKT alebo ich používateľov, najmä MSP;

iv) zohľadní existenciu a vykonávanie príslušných právnych predpisov členského štátu.

3. Komisia môže požiadať agentúru ENISA, aby vypracovala kandidátsky systém **alebo preskúmala existujúci európsky systém certifikácie kybernetickej bezpečnosti** podľa článku 48 ods. 2 nariadenia (EÚ) 2019/881 v prípadoch, keď nie je k dispozícii žiadny európsky systém certifikácie kybernetickej bezpečnosti na účely odseku 2 **tohto článku**.

Článok 22

Normalizácia

1. Členské štáty v záujme harmonizovaného vykonávania článku 18 ods. 1 a 2 a bez toho, aby ukladali povinnosť využívať určitý typ technológie alebo diskriminovali v prospech takéhoto využívania, podporujú využívanie európskych alebo medzinárodne uznávaných noriem a špecifikácií, ktoré sú relevantné pre bezpečnosť sietí a informačných systémov.

2. Agentúra ENISA v spolupráci s členskými štátmi vypracúva odporúčania a usmernenia týkajúce sa technických oblastí, ktoré sa majú zvážiť v súvislosti s odsekom 1, ako aj odporúčania a usmernenia týkajúce sa už existujúcich noriem vrátane vnútroštátnych noriem členských štátov, ktoré by sa mohli vzťahovať na uvedené oblasti.

Článok 23

Databázy doménových mien a registračných údajov

1. S cieľom prispieť k bezpečnosti, stabilite a odolnosti DNS členské štáty zabezpečia, aby správcovia **mien** TLD a subjekty poskytujúce služby registrácie doménových mien pre TLD zbierali a uchovávali presné **[...] a** úplné registračné údaje o doménových menách vo vyhradenom databázovom zariadení s náležitou starostlivosťou v **súlade s** právnymi predpismi Únie o ochrane údajov, pokiaľ ide o údaje, ktoré sú osobnými údajmi.

2. Členské štáty zabezpečia, aby databázy s registračnými údajmi o doménových menách uvedené v odseku 1 obsahovali relevantné informácie na identifikáciu a kontaktovanie držiteľov doménových mien a kontaktných miest spravujúcich doménové mená v rámci TLD**, a to prinajmenšom tieto údaje:**

   a) meno domény;

   b) dátum registrácie;

   c) údaje o držiteľovi domény vrátane:

      i) v prípade fyzických osôb – meno, priezvisko a e-mailová adresa;

      ii) v prípade právnických osôb – názov a e-mailová adresa.

3. Členské štáty zabezpečia, aby správcovia **mien** TLD a subjekty poskytujúce služby registrácie doménových mien pre TLD mali zavedené politiky a postupy s cieľom zabezpečiť, aby databázy obsahovali presné a úplné informácie. Členské štáty zabezpečia, aby takéto politiky a postupy boli verejne dostupné.

4. Členské štáty zabezpečia, aby správcovia **mien** TLD a subjekty poskytujúce služby registrácie doménových mien pre TLD bez zbytočného odkladu po registrácii mena domény uverejnili registračné údaje domény, ktoré nie sú osobnými údajmi.

5. Členské štáty zabezpečia, aby správcovia **mien** TLD a subjekty poskytujúce služby registrácie doménových mien pre TLD poskytovali prístup k špecifickým registračným údajom o doménových menách na základe zákonných a riadne odôvodnených žiadostí oprávnených záujemcov o prístup v súlade s právnymi predpismi Únie o ochrane údajov. Členské štáty zabezpečia, aby správcovia **mien** TLD a subjekty poskytujúce služby registrácie doménových mien pre TLD odpovedali bez zbytočného odkladu**, najneskôr však do 72 hodín,** na všetky žiadosti o prístup. Členské štáty zabezpečia, aby politiky a postupy zverejňovania takýchto údajov boli verejne dostupné. Oddiel II Jurisdikcia a registrácia Článok 24 Jurisdikcia a teritorialita

Oddiel II

Právomoc a registrácia

Článok 24

Právomoc a teritorialita

1a. O subjektoch, na ktoré sa vzťahuje táto smernica, platí, že podliehajú právomoci toho členského štátu, v ktorom poskytujú svoje služby. O subjektoch uvedených v bodoch 1 až 7 a 10 prílohy I, o poskytovateľoch dôveryhodných služieb a o poskytovateľoch internetových prepojovacích uzlov uvedených v bode 8 prílohy I a bodoch 1 až 5 prílohy II platí, že podliehajúce právomoci toho členského štátu, na ktorého území sú usadené.

1. O poskytovateľoch služieb DNS, správcoch mien TLD [...] a **subjektoch, ktoré poskytujú služby registrácie doménových mien pre TLD**, poskytovateľoch služieb cloud computingu, poskytovateľoch služieb dátového centra, [...] poskytovateľoch sietí na sprístupňovanie obsahu, **poskytovateľoch riadených služieb a poskytovateľoch riadených bezpečnostných služieb** uvedených v bodoch 8 a **8a** prílohy I, ako aj o poskytovateľoch digitálnych služieb uvedených v bode 6 prílohy II platí, že podliehajú právomoci členského štátu, v ktorom majú hlavné miesto podnikateľskej činnosti v Únii.

2. Na účely tejto smernice platí, že subjekty uvedené v odseku 1 majú hlavné miesto podnikateľskej činnosti v Únii v členskom štáte, v ktorom sa **najčastejšie** prijímajú rozhodnutia týkajúce sa opatrení na riadenie kybernetickobezpečnostných rizík. Ak **nie je možné určiť miesto, v ktorom sa takéto rozhodnutia prijímajú najčastejšie, alebo ak** sa takéto rozhodnutia neprijímajú v žiadnom mieste podnikateľskej činnosti v Únii, platí, že hlavné miesto podnikateľskej činnosti je v členskom štáte, v ktorom majú subjekty miesto podnikateľskej činnosti s najvyšším počtom zamestnancov v Únii. **Ak služby poskytuje skupina podnikov, za hlavné miesto podnikateľskej činnosti sa považuje hlavné miesto podnikateľskej činnosti skupiny podnikov.**

3. Ak subjekt uvedený v odseku 1 nie je usadený v Únii, ale ponúka služby v rámci Únie, určí zástupcu v Únii. Zástupca musí byť usadený v jednom z členských štátov, v ktorých ponúka služby. Predpokladá sa, že takýto subjekt podlieha jurisdikcii toho členského štátu, v ktorom je usadený jeho zástupca. Ak v zmysle tohto článku nie je v Únii určený zástupca, ktorýkoľvek členský štát, v ktorom subjekt poskytuje služby, môže proti tomuto subjektu podniknúť právne kroky pre nedodržanie povinností podľa tejto smernice.

4. Ak subjekt určí zástupcu v zmysle odseku 1, nie sú tým dotknuté právne kroky, ktoré by mohli byť podniknuté proti samotnému subjektu.

4a. Členské štáty, ktorým bola doručená žiadosť o vzájomnú pomoc vo vzťahu k subjektom uvedeným v odseku 1, môžu v medziach žiadosti prijať primerané opatrenia v oblasti dohľadu a presadzovania vo vzťahu k dotknutému subjektu, ktorý poskytuje služby alebo ktorý má sieť a informačný systém na ich území.

Článok 25

Register určitých subjektov digitálnej infraštruktúry a poskytovateľov digitálnych služieb

1. [...] **Členské štáty zabezpečia, aby** [...] subjekty **uvedené v článku 24 ods. 1, ktoré majú hlavné miesto podnikateľskej činnosti ich území alebo ktoré v prípade, že nie sú usadené v Únii, majú v Únii určeného zástupcu usadeného na ich území, mali povinnosť** [...] predložiť **príslušným orgánom** [...] [najneskôr do 12 mesiacov od nadobudnutia účinnosti tejto smernice] tieto informácie:

a) názov subjektu;

aa) typ subjektu podľa príloh I a II k tejto smernici;

b) adresu svojho hlavného miesta podnikateľskej činnosti a iných zákonných miest podnikateľskej činnosti v Únii, alebo ak nie sú usadené v Únii, adresu svojho zástupcu určeného podľa článku 24 ods. 3;

c) aktuálne kontaktné údaje vrátane e-mailových adries a telefónnych čísel subjektov a **ich zástupcov;**

d) členské štáty, v ktorých subjekt poskytuje službu.

V náležitom prípade sa tieto informácie predkladajú prostredníctvom vnútroštátneho mechanizmu [...] oznamovania vlastných údajov uvedeného v článku 2a.

2. **Členské štáty zabezpečia, aby** [...] subjekty uvedené v odseku 1 [...] **oznámili aj** všetky zmeny údajov, ktoré predložili podľa odseku 1, a to bezodkladne a v každom prípade do troch mesiacov odo dňa, keď zmena nadobudla účinnosť.

3. [...] **Jednotné kontaktné miesta členských štátov** postúpia **informácie uvedené v odsekoch 1 a 2** [...] [...] **agentúre ENISA**. [...]

3a. Na základe informácií získaných podľa odseku 3 tohto článku agentúra ENISA vytvorí a vedie register subjektov uvedených v odseku 1. Agentúra ENISA na žiadosť členských štátov umožní prístup relevantných príslušných orgánov do registra, pričom v náležitom prípade zabezpečí potrebné záruky na ochranu dôvernosti informácií.

4. [...]

KAPITOLA V

Zdieľanie informácií

Článok 26

Dojednania o zdieľaní informácií o kybernetickej bezpečnosti

1. [...] Členské štáty zabezpečia, aby si kľúčové a dôležité subjekty mohli medzi sebou na **dobrovoľnej báze** vymieňať relevantné informácie o kybernetickej bezpečnosti vrátane informácií o kybernetických hrozbách, **odvrátených udalostí**, zraniteľnostiach, ukazovateľoch kompromitácie, taktikách, technikách a postupoch, kybernetickobezpečnostných varovaniach a konfiguračných nástrojoch, ak takáto výmena informácií:

   a) má za cieľ predchádzať incidentom, odhaľovať ich, reagovať na ne alebo ich zmierňovať;

b) zvyšuje úroveň kybernetickej bezpečnosti, najmä zvyšovaním povedomia o kybernetických hrozbách, obmedzovaním alebo zabraňovaním možnosti šírenia takýchto hrozieb, podporou celej škály obranných kapacít, zverejňovaním informácií o zraniteľnosti a jej nápravou, technikami odhaľovania hrozieb, stratégiami zmierňovania, alebo fázami reakcie a obnovy.

2. Členské štáty zabezpečia, aby sa výmena informácií uskutočňovala v rámci [...] komunít kľúčových a dôležitých subjektov. Takáto výmena sa uskutočňuje prostredníctvom dojednaní o zdieľaní informácií vzhľadom na potenciálne citlivú povahu zdieľaných informácií [...].

3. Členské štáty [...] **môžu** stanoviť pravidlá, v ktorých sa konkretizuje postup, operačné prvky (vrátane využívania špecializovaných platforiem IKT), obsah a podmienky dojednaní o zdieľaní informácií uvedených v odseku 2. V týchto pravidlách [...] **sa môžu** stanoviť aj podrobnosti o zapojení orgánov verejnej moci do takýchto dojednaní, ako aj operačné prvky vrátane využívania špecializovaných IT platforiem. Členské štáty poskytnú pri uplatňovaní takýchto dojednaní podporu v súlade so svojimi politikami uvedenými v článku 5 ods. 2 písm. g).

4. Kľúčové a dôležité subjekty oznámia príslušným orgánom svoju účasť na dojednaniach o zdieľaní informácií uvedených v odseku 2 pri uzatváraní takýchto dojednaní alebo prípadne ich odstúpení od takýchto dojednaní, keď odstúpenie nadobudne účinnosť.

5. Agentúra ENISA podporuje [...] uzavretie dojednaní o zdieľaní informácií o kybernetickej bezpečnosti uvedených v odseku 2 poskytovaním najlepších postupov a usmernení.

Článok 27

Dobrovoľné oznamovanie relevantných informácií

1. Bez toho, aby bol dotknutý článok 20, členské štáty zabezpečia, aby kľúčové a dôležité subjekty mohli dobrovoľne oznamovať príslušným orgánom alebo jednotkám CSIRT všetky relevantné incidenty, kybernetické hrozby alebo odvrátené udalosti.

2. Členské štáty zabezpečia, aby subjekty, ktoré nepatria do rozsahu pôsobnosti tejto smernice, mohli dobrovoľne podávať oznámenia o závažných incidentoch, kybernetických hrozbách alebo udalostiach odvrátených v poslednej chvíli, a to bez toho, aby bol dotknutý článok 3. Členské štáty pri spracúvaní oznámení konajú v súlade s postupom stanoveným v článku 20. Členské štáty môžu uprednostniť spracúvanie povinných oznámení pred dobrovoľnými oznámeniami. **Bez toho, aby bolo dotknuté 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.

3. Dobrovoľné oznámenia sa spracúvajú len vtedy, ak takéto spracovanie nepredstavuje neprimerané alebo nenáležité zaťaženie dotknutého členského štátu.

KAPITOLA VI

Dohľad a presadzovanie práva

Článok 28

Všeobecné aspekty týkajúce sa dohľadu a presadzovania práva

1. Členské štáty zabezpečia, aby príslušné orgány účinne monitorovali a prijímali opatrenia potrebné na zabezpečenie súladu s touto smernicou, najmä s povinnosťami stanovenými v článkoch 18**,** [...] 20 a **23**. **Členské štáty môžu príslušným orgánom povoliť, aby uprednostnili dohľad, ktorý vychádza z prístupu založeného na riziku.**

2. Keď príslušné orgány riešia kybernetickobezpečnostné incidenty, úzko spolupracujú s orgánmi pre ochranu údajov, **príslušnými orgánmi určenými podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov], dozornými orgánmi určenými podľa nariadenia (EÚ) 910/2014 a inými príslušnými orgánmi určenými podľa právnych aktov Únie platných pre jednotlivé odvetvia.** [...]

3. Bez toho, aby boli dotknuté vnútroštátne legislatívne a inštitucionálne rámce, členské štáty zabezpečia, aby príslušné orgány mali pri dohľade nad dodržiavaním tejto smernice zo strany subjektov verejnej správy a pri presadzovaní prípadných sankcií za jej nedodržiavanie primerané právomoci na plnenie takýchto úloh s operačnou nezávislosťou od dohliadaných subjektov. Členské štáty môžu rozhodnúť o uložení vhodných, primeraných a účinných opatrení dohľadu a presadzovania vo vzťahu k týmto subjektom v súlade s vnútroštátnymi rámcami a právnym poriadkom.

Článok 29

Dohľad a presadzovanie práva v prípade 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, pričom zohľadnia okolnosti každého jednotlivého prípadu.

2. Členské štáty zabezpečia, aby príslušné orgány pri vykonávaní svojich úloh dohľadu nad kľúčovými subjektmi **uplatňovali prístup založený na riziku** a mali právomoc podrobiť tieto subjekty **prinajmenšom**:

   a) kontrolám na mieste a dohľadu na diaľku vrátane náhodných kontrol;

   b) pravidelným **bezpečnostným** auditom;

   c) cieleným bezpečnostným auditom založeným na posúdeniach rizika alebo dostupných informáciách súvisiacich s rizikom;

   d) bezpečnostným kontrolám založeným na objektívnych, nediskriminačných, spravodlivých a transparentných kritériách posúdenia rizika v **spolupráci s dotknutým subjektom, ak je to potrebné z technických dôvodov**;

   e) žiadostiam o informácie potrebné na posúdenie kybernetickobezpečnostných opatrení, ktoré subjekt prijal, vrátane zdokumentovaných politík v oblasti kybernetickej bezpečnosti [...];

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

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

2a. Príslušné orgány môžu pri vykonávaní svojich úloh dohľadu stanovených v odseku 2 tohto článku stanoviť metodiky dohľadu, ktoré umožnia uprednostnenie takýchto úloh na základe prístupu založeného na riziku.

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

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

a) vydávať varovania, že subjekty nedodržiavajú povinnosti stanovené v tejto smernici;

b) vydávať záväzné pokyny alebo príkazy, ktorými sa od týchto subjektov vyžaduje napraviť zistené nedostatky alebo porušenia povinností stanovených v tejto smernici;

c) nariadiť týmto subjektom, aby upustili od konania, ktoré nie je v súlade s povinnosťami stanovenými v tejto smernici, a zdržať sa opakovania takého konania;

d) nariadiť týmto subjektom, aby svoje opatrenia na riadenie rizík a/alebo oznamovacie povinnosti zosúladili s povinnosťami stanovenými v článkoch 18 a 20 určeným spôsobom a v určenej lehote;

e) nariadiť týmto subjektom, aby informovali fyzické alebo právnické osoby, ktorým poskytujú služby alebo činnosti, ktoré sú potenciálne zasiahnuté závažnou 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 týmto subjektom, aby v primeranej lehote vykonali odporúčania poskytnuté na základe bezpečnostného auditu;

g) [...]

h) nariadiť týmto subjektom, aby určeným spôsobom zverejnili aspekty nedodržiavania povinností stanovených v tejto smernici**, ak takéto zverejnenie nevedie k škodlivej expozícii príslušného subjektu**;

i) [...]

j) uložiť správnu sankciu alebo požiadať o jej uloženie podľa článku 31 príslušné orgány alebo súdy podľa vnútroštátnych zákonov, a to popri opatreniach uvedených v písmenách a) až i) tohto odseku alebo namiesto týchto opatrení, v závislosti od okolností každého jednotlivého prípadu.

5. Ak sa opatrenia na presadzovanie práva prijaté podľa odseku 4 písm. a) až d) a f) ukážu ako neúčinné, členské štáty zabezpečia, aby príslušné orgány mali právomoc stanoviť lehotu, v 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 príslušné orgány mali právomoc:

a) pozastaviť certifikáciu alebo povoľovanie alebo požiadať certifikačný alebo povoľujúci subjekt**, prípadne súdy podľa vnútroštátneho práva**, aby pozastavil certifikáciu alebo povoľovanie týkajúce sa časti alebo všetkých služieb alebo činností, ktoré poskytuje kľúčový subjekt;

b) uložiť dočasný zákaz alebo od príslušných orgánov alebo súdov podľa vnútroštátnych zákonov požadovať uloženie dočasného zákazu vykonávať riadiace funkcie v tomto kľúčovom subjekte, a to každej osobe vykonávajúcej riadiace úlohy na úrovni výkonného riaditeľa alebo právneho zástupcu v tomto kľúčovom subjekte a akejkoľvek inej fyzickej osobe zodpovednej za porušenie.

Tieto sankcie sa uplatňujú len dovtedy, kým subjekt neprijme potrebné opatrenia na nápravu nedostatkov alebo nesplní požiadavky príslušného orgánu, ktorý takéto sankcie uplatnil.

Sankcie stanovené v tomto odseku sa nevzťahujú 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 zástupca na základe právomoci zastupovať ho, prijímať rozhodnutia v jeho mene alebo vykonávať kontrolu nad ním mala právomoc zabezpečiť dodržiavanie povinností stanovených v tejto smernici. Členské štáty zabezpečia, aby tieto fyzické osoby mohli niesť zodpovednosť za porušenie svojich úloh zabezpečovať dodržiavanie povinností stanovených v tejto smernici. **Pokiaľ ide o subjekty verejnej správy, týmto ustanovením nie sú dotknuté právne predpisy členských štátov, pokiaľ ide o zodpovednosť štátnych zamestnancov a volených a vymenovaných úradníkov.**

7. Príslušné orgány pri prijímaní opatrení na presadzovanie práva alebo uplatňovaní sankcií podľa odsekov 4 a 5 dodržiavajú právo na obhajobu a zohľadňujú okolnosti každého jednotlivého prípadu a prinajmenšom náležite zohľadňujú:

   a) závažnosť porušenia a dôležitosť porušených ustanovení. Medzi porušenia, ktoré by sa mali považovať za závažné, patria: opakované porušenia, neoznámenie incidentov so závažným účinkom narušenia alebo nevykonanie ich nápravy, nevykonanie nápravy nedostatkov na základe záväzných pokynov príslušných orgánov, marenie auditov alebo monitorovacích činností nariadených príslušným orgánom na základe zistenia porušenia, poskytovanie nepravdivých alebo hrubo nepresných informácií týkajúcich sa požiadaviek na riadenie rizík alebo oznamovacích povinností stanovených v článkoch 18 a 20;

b) trvanie porušenia vrátane opakovaného porušovania;

c) skutočné spôsobené škody alebo vzniknuté straty alebo potenciálne škody alebo straty, ktoré mohli vzniknúť, pokiaľ ich možno určiť. Pri hodnotení tohto aspektu sa okrem iného zohľadnia skutočné alebo potenciálne finančné alebo hospodárske straty, účinky na iné služby, počet dotknutých alebo potenciálne dotknutých používateľov;

d) úmyselný alebo nedbanlivostný charakter porušenia;

e) opatrenia, ktoré subjekt prijal na zabránenie alebo zmiernenie škôd a/alebo strát;

f) dodržiavanie schválených kódexov správania alebo schválených mechanizmov certifikácie;

g) úroveň spolupráce zodpovednej fyzickej alebo právnickej osoby (osôb) s príslušnými orgánmi.

8. Príslušné orgány uvedú podrobné odôvodnenie svojich rozhodnutí na presadzovanie práva. Pred prijatím takýchto rozhodnutí oznámia dotknutým subjektom svoje predbežné zistenia a v prípade, že **nehrozí bezprostredné nebezpečenstvo**, im poskytnú primeraný čas na predloženie pripomienok.

9. Členské štáty zabezpečia, aby ich príslušné orgány **podľa tejto smernice** informovali relevantné príslušné orgány v **tom istom** [...] členskom štáte [...] určené podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov], keď vykonávajú svoje právomocí v oblasti dohľadu a presadzovania zamerané na zabezpečenie dodržiavania povinností podľa tejto smernice zo strany kľúčového subjektu identifikovaného ako kritický **[**alebo ako rovnocenný s kritickým subjektom**]** podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov]. [...] Príslušné orgány podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov] [...] **môžu v náležitých prípadoch požiadať** príslušné orgány **podľa tejto smernice** [...], aby vykonávali ich **právomoci** v oblasti dohľadu a presadzovania vo **vzťahu ku** kľúčovému subjektu, ktorý patrí do rozsahu pôsobnosti tejto smernice a ktorý je tiež identifikovaný ako kritický subjekt **[**alebo jeho ekvivalent**] podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov].**

10. Členské štáty zabezpečia, aby ich príslušné orgány podľa tejto smernice informovali fórum pre dozor podľa článku 29 ods. 1 nariadenia (EÚ) XXXX/XXXX [DORA] pri výkone svojich právomocí v oblasti dohľadu a presadzovania zameraných na zabezpečenie dodržiavania povinností podľa tejto smernice zo strany kľúčového subjektu označeného ako externý poskytovateľ kritických služieb IKT podľa článku 28 nariadenia (EÚ) XXXX/XXXX [DORA].

10a. Členské štáty zabezpečia, aby ich príslušné orgány podľa tejto smernice informovali relevantné príslušné orgány určené podľa nariadenia (EÚ) č. 910/2014, keď vykonávajú svoje právomocí v oblasti dohľadu a presadzovania, ktorých cieľom je zabezpečiť, aby subjekt označený ako poskytovateľ dôveryhodných služieb podľa nariadenia (EÚ) č. 910/2014 dodržiaval povinnosti podľa tejto smernice.

Článok 30

Dohľad a presadzovanie práva v prípade dôležitých subjektov

1. Ak členské štáty dostanú dôkaz, indíciu **alebo informáciu**, že dôležitý subjekt **údajne** nedodržiava povinnosti stanovené v tejto smernici, a najmä v článkoch 18 a 20, zabezpečia, aby príslušné orgány konali v prípade potreby prostredníctvom opatrení dohľadu *ex post*.

2. Členské štáty zabezpečia, aby príslušné orgány pri vykonávaní svojich úloh dohľadu nad dôležitými subjektmi **uplatňovali prístup založený na riziku a** mali právomoc podrobiť tieto subjekty **prinajmenšom**:

   a) kontrolám na mieste a dohľadu ex post na diaľku;

   b) cieleným bezpečnostným auditom založeným na posúdeniach rizika alebo dostupných informáciách súvisiacich s rizikom;

   c) bezpečnostným kontrolám založeným na objektívnych, **nediskriminačných,** spravodlivých a transparentných kritériách posúdenia rizika v **spolupráci s dotknutým subjektom, ak je to potrebné z technických dôvodov**;

   d) žiadostiam o informácie potrebné na posúdenie ex post týkajúce sa opatrení v oblasti kybernetickej [...];

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

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

2a. Príslušné orgány môžu pri vykonávaní svojich úloh dohľadu stanovených v odseku 2 tohto článku stanoviť metodiky dohľadu, ktoré umožnia uprednostnenie takýchto úloh na základe prístupu založeného na riziku.

3. Príslušné orgány pri vykonávaní svojich právomocí podľa odseku 2 písm. d) **až ea)** uvedú účel žiadosti a konkretizujú požadované informácie.

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

a) vydávať varovania, že subjekty nedodržiavajú povinnosti stanovené v tejto smernici;

b) vydávať záväzné pokyny alebo príkazy, ktorými sa od týchto subjektov vyžaduje napraviť zistené nedostatky alebo porušenie povinností stanovených v tejto smernici;

c) nariadiť týmto subjektom, aby upustili od konania, ktoré nie je v súlade s povinnosťami stanovenými v tejto smernici, a zdržať sa opakovania takého konania;

d) nariadiť týmto subjektom, aby svoje opatrenia na riadenie rizík alebo oznamovacie povinnosti zosúladili s povinnosťami stanovenými v článkoch 18 a 20 určeným spôsobom a v určenej lehote;

e) nariadiť týmto subjektom, aby informovali fyzické alebo právnické osoby, ktorým poskytujú služby alebo činnosti, ktoré sú potenciálne zasiahnuté závažnou 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 týmto subjektom, aby v primeranej lehote vykonali odporúčania poskytnuté na základe bezpečnostného auditu;

g) nariadiť týmto subjektom, aby určeným spôsobom zverejnili aspekty nedodržiavania svojich povinností stanovených v tejto smernici**, ak takéto zverejnenie nevedie k škodlivej expozícii príslušného subjektu**;

h) [...]

i) uložiť správnu sankciu alebo požiadať o jej uloženie podľa článku 31 príslušné orgány alebo súdy podľa vnútroštátnych zákonov, a to popri opatreniach uvedených v písmenách a) až h) tohto odseku alebo namiesto týchto opatrení, v závislosti od okolností každého jednotlivého prípadu.

5. Článok 29 ods. 6 až 8 sa uplatňuje aj na opatrenia dohľadu a presadzovania stanovené v tomto článku v prípade dôležitých subjektov [...].

Článok 31

Všeobecné podmienky ukladania správnych sankcií kľúčovým a dôležitým subjektom

1. Členské štáty zabezpečia, aby uloženie správnych sankcií kľúčovým a dôležitým subjektom podľa tohto článku za porušenie povinností stanovených v tejto smernici bolo v každom jednotlivom prípade účinné, primerané a odrádzajúce.

2. Správne sankcie sa v závislosti od okolností každého jednotlivého prípadu ukladajú popri opatreniach uvedených v článku 29 ods. 4 písm. a) až i), článku 29 ods. 5 a článku 30 ods. 4 písm. a) až h) a j) alebo namiesto týchto opatrení.

3. Pri rozhodovaní o uložení správnej sankcie, ako aj pri rozhodovaní o jej výške v každom jednotlivom prípade sa náležite zohľadnia aspoň prvky stanovené v článku 29 ods. 7.

4. Členské štáty zabezpečia, aby sa v prípade, keď **kľúčové subjekty** porušia povinnosti stanovené v článku 18 alebo článku 20, uložili v súlade s odsekmi 2 a 3 tohto článku správne pokuty v maximálnej výške aspoň **4**[...] 000 000 EUR alebo v **prípade právnickej osoby** [...] 2 % celkového svetového ročného obratu podniku, ku ktorému kľúčový [...] subjekt patrí, v predchádzajúcom hospodárskom roku, podľa toho, ktorá suma je vyššia.

4a. Členské štáty zabezpečia, aby sa v prípade, keď dôležité subjekty porušia povinnosti stanovené v článku 18 alebo článku 20, uložili v súlade s odsekmi 2 a 3 tohto článku správne pokuty v maximálnej výške aspoň 2 000 000 EUR alebo v prípade právnickej osoby 1 % celkového svetového ročného obratu podniku, ku ktorému dôležitý subjekt patrí, v predchádzajúcom hospodárskom roku, podľa toho, ktorá suma je vyššia.

5. Členské štáty môžu v súlade s predchádzajúcim rozhodnutím príslušného orgánu stanoviť právomoc ukladať pravidelné peňažné pokuty s cieľom prinútiť kľúčový alebo dôležitý subjekt, aby prestal porušovať predpisy.

6. Bez toho, aby boli dotknuté právomoci príslušných orgánov podľa článkov 29 a 30, každý členský štát môže stanoviť pravidlá, či a v akom rozsahu sa môžu správne sankcie uložiť subjektom verejnej správy uvedeným v článku 4 bode 23 s prihliadnutím na povinnosti stanovené v tejto smernici.

6a. Ak sa v právnom systéme členského štátu nestanovujú správne pokuty, členské štáty zabezpečia, aby sa tento článok mohol uplatňovať tak, že uloženie pokuty iniciuje príslušný orgán a uloží ju príslušný vnútroštátny súd, 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. Uvedené členské štáty oznámia ustanovenia svojich právnych predpisov, ktoré prijmú podľa tohto odseku, Komisii do [...] a bezodkladne oznámia aj všetky následné pozmeňujúce právne predpisy či zmeny, ktoré sa ich týkajú.

Článok 32

Porušenia povinností, pri ktorých došlo k porušeniu ochrany osobných údajov

1. Ak príslušné orgány **nadobudnú počas výkonu dohľadu alebo presadzovania vedomie** [...], že porušenie povinností stanovených v článkoch 18 a 20 **tejto smernice** zo strany kľúčového alebo dôležitého subjektu **môže** spôsobiť [...] porušenie ochrany osobných údajov, ako sa vymedzuje 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 príslušné dozorné orgány podľa článkov 55 a 56 uvedeného nariadenia.

2. Ak sa dozorné orgány, ktoré sú príslušné v súlade s článkami 55 a 56 nariadenia (EÚ) 2016/679, rozhodnú uplatniť svoje právomoci podľa článku 58 **ods. 2** písm. i) uvedeného nariadenia a uložiť správnu pokutu, príslušné orgány **uvedené v článku 8 tejto smernice** neuložia správnu pokutu pre [...] **ten istý skutok, ktorý je** porušením **podľa** [...] článku 31 tejto smernice. Príslušné orgány však môžu uplatňovať opatrenia na presadzovanie práva alebo vykonávať sankčné právomoci stanovené v článku 29 ods. 4 písm. a) až i), článku 29 ods. 5 a článku 30 ods. 4 písm. a) až h) tejto smernice.

3. Ak je dozorný orgán, príslušný podľa nariadenia (EÚ) 2016/679, usadený v inom členskom štáte než príslušný orgán, príslušný orgán môže informovať dozorný orgán usadený v tom istom členskom štáte.

Článok 33

Sankcie

1. Členské štáty stanovia pravidlá ukladania sankcií za porušenie vnútroštátnych predpisov prijatých podľa tejto smernice a prijmú všetky opatrenia potrebné na zabezpečenie ich uplatňovania. Stanovené sankcie musia byť účinné, primerané a odrádzajúce.

2. Členské štáty najneskôr do [dvoch] rokov od nadobudnutia účinnosti tejto smernice oznámia tieto pravidlá a opatrenia Komisii a bez zbytočného odkladu jej oznámia všetky následné zmeny, ktoré sa ich týkajú.

Článok 34

Vzájomná pomoc

1. Ak kľúčový alebo dôležitý subjekt poskytuje služby vo viac ako jednom členskom štáte, alebo [...] **poskytuje služby v jednom alebo viacerých** členských štátoch, ale jeho siete a informačné systémy sú umiestnené v niektorom inom alebo vo viacerých iných členských štátoch, príslušné orgány [...] **dotknutého** členského štátu [...] spolupracujú a v prípade potreby si navzájom pomáhajú. Táto spolupráca zahŕňa aspoň tieto prvky:

a) príslušné orgány, ktoré uplatňujú opatrenia v oblasti 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 v oblasti 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 pomoc **primeranú zdrojom, ktoré má k dispozícii**, aby sa opatrenia dohľadu alebo presadzovania práva [...] mohli vykonávať účinným, efektívnym a konzistentným spôsobom. Takáto vzájomná pomoc sa môže vzťahovať na žiadosti o informácie a opatrenia dohľadu vrátane žiadostí o vykonanie kontrol na mieste alebo dohľadu na diaľku alebo cielených bezpečnostných auditov. Príslušný orgán, ktorému je žiadosť o pomoc určená, nesmie túto žiadosť zamietnuť, pokiaľ sa po výmene názorov s ostatnými dotknutými orgánmi[...] nestanoví, že [...] daný orgán nie je príslušný poskytnúť požadovanú pomoc **alebo nemá potrebné zdroje**, alebo že požadovaná pomoc nie je primeraná vykonávaným úlohám príslušného orgánu v oblasti dohľadu [...], **alebo že sa žiadosť týka informácií alebo vyžaduje činnosti, ktoré sú v rozpore s národnou bezpečnosťou, verejnou bezpečnosťou alebo obranou daného členského štátu**.

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

KAPITOLA VII

Prechodné a záverečné ustanovenia

Článok 35

Preskúmanie

Komisia pravidelne preskúmava fungovanie tejto smernice a podáva o tom správu Európskemu parlamentu a Rade. V správe sa posúdi najmä relevantnosť odvetví, pododvetví, veľkosti a typu subjektov uvedených v prílohách I a II pre fungovanie hospodárstva a spoločnosti v súvislosti s kybernetickou bezpečnosťou. Na [...] účely **preskúmania** [...] Komisia zohľadní správy [...] siete jednotiek CSIRT o skúsenostiach získaných na [...] operačnej úrovni. Prvá správa sa predloží do … [54 mesiacov po dátume nadobudnutia účinnosti tejto smernice].

Článok 36

[...]

[...]

[...]

Článok 37

Postup výboru

1. Komisii pomáha výbor. Uvedený výbor je výborom v zmysle nariadenia (EÚ) č. 182/2011.

2. Ak sa odkazuje na tento odsek, uplatňuje sa článok 5 nariadenia (EÚ) č. 182/2011.

3. Ak sa má stanovisko výboru získať písomným postupom, tento postup sa ukončí bez výsledku, ak tak v rámci lehoty na vydanie stanoviska rozhodne predseda výboru alebo ak o to požiada člen výboru.

Článok 38

Transpozícia

1. Členské štáty prijmú a uverejnia [...] zákony, iné právne predpisy a správne opatrenia potrebné na dosiahnutie súladu s touto smernicou do [[...]**24** mesiacov od nadobudnutia jej účinnosti**]**. Bezodkladne o tom informujú Komisiu. Tieto ustanovenia sa uplatňujú od … [jeden deň po dátume uvedenom v prvom pododseku].

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

Článok 39

Zmena nariadenia (EÚ) č. 910/2014

Z nariadenia (EÚ) č. 910/2014 sa vypúšťa článok 19 [...]**, a to s účinnosťou od ... [dátum lehoty na transpozíciu tejto smernice].**

Článok 40

Zmena smernice (EÚ) 2018/1972

Zo smernice (EÚ) 2018/1972 sa vypúšťajú články 40 a 41 [...], a **to s účinnosťou od ... [dátum lehoty na transpozíciu tejto smernice]**.

Článok 41

Zrušenie

Smernica (EÚ) 2016/1148 sa zrušuje s účinnosťou od ... [dátum lehoty na transpozíciu smernice].

Odkazy na smernicu (EÚ) 2016/1148 sa považujú za odkazy na túto smernicu a znejú v súlade s tabuľkou zhody uvedenou v prílohe II[...].

Článok 42

Nadobudnutie účinnosti

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

Článok 43

Adresáti

Táto smernica je určená členským štátom.

V Bruseli

Za Európsky parlament	*Za Radu*
predseda	*predseda*

PRÍLOHA I

ODVETVIA, PODODVETVIA A TYPY SUBJEKTOV

Odvetvie	Pododvetvie	Typ subjektu
1. Energetika	a) Elektrická energia	— elektroenergetické podniky uvedené v článku 2 bode 57 smernice (EÚ) 2019/944, ktoré vykonávajú funkciu „dodávky“ podľa vymedzenia v článku 2 bode 12 uvedenej smernice ([39])
		— prevádzkovatelia distribučnej sústavy uvedení v článku 2 bode 29 smernice (EÚ) 2019/944
		— prevádzkovatelia prenosovej sústavy uvedení v článku 2 bode 35 smernice (EÚ) 2019/944
		— výrobcovia uvedení v článku 2 bode 38 smernice (EÚ) 2019/944
		— nominovaní organizátori trhu s elektrinou uvedení v článku 2 bode 8 nariadenia (EÚ) 2019/943 ([40])
		— účastníci trhu s elektrinou uvedení v článku 2 bode 25 nariadenia (EÚ) 2019/943, ktorí poskytujú služby agregácie, riadenia odberu alebo uskladňovania energie uvedené v článku 2 bodoch 18, 20 a 59 smernice (EÚ) 2019/944

[39] 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).

[40] Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/943 o vnútornom trhu s elektrinou (Ú. v. EÚ L 158, 14.6.2019, s. 54).

	b) Diaľkové vykurovanie a chladenie	— diaľkové vykurovanie alebo diaľkové chladenie uvedené v článku 2 bode 19 smernice (EÚ) 2018/2001 ([41]) o podpore využívania energie z obnoviteľných zdrojov
	c) Ropa	— prevádzkovatelia ropovodov
		— prevádzkovatelia zariadení na ťažbu, rafinovanie a spracovanie ropy, jej skladovanie a prepravu
		— ústredné subjekty správy zásob ropy uvedené v článku 2 písm. f) smernice Rady 2009/119/ES ([42])
	d) Plyn	— dodávateľské podniky uvedené v článku 2 bode 8 smernice (EÚ) 2009/73/ES ([43])
		— prevádzkovatelia distribučnej siete uvedení v článku 2 bode 6 smernice 2009/73/ES
		— prevádzkovatelia prepravnej siete uvedení v článku 2 bode 4 smernice 2009/73/ES
		— prevádzkovatelia zásobníkov uvedení v článku 2 bode 10 smernice 2009/73/ES
		— prevádzkovatelia zariadenia LNG

[41] 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).

[42] 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).

[43] 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).

		uvedení v článku 2 bode 12 smernice 2009/73/ES
		— plynárenské podniky uvedené 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
2. Doprava	a) Letecká doprava	— leteckí dopravcovia uvedení v článku 3 bode 4 nariadenia (ES) č. 300/2008 ([44]) **využívaní na komerčné účely**
		— riadiace orgány letiska uvedené v článku 2 bode 2 smernice 2009/12/ES([45]), letiská uvedené v článku 2 bode 1 uvedenej smernice vrátane hlavných letísk uvedených v oddiele 2 prílohy II k nariadeniu (EÚ) č. 1315/2013 ([46]) a subjekty prevádzkujúce pomocné zariadenia nachádzajúce sa na letiskách
		— prevádzkovatelia poskytujúci služby riadenia letovej prevádzky (ATC)

[44] 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).

[45] 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).

[46] 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).

		uvedení v článku 2 bode 1 nariadenia (ES) č. 549/2004 ([47])
	b) Železničná doprava	— manažéri infraštruktúry uvedení v článku 3 bode 2 smernice 2012/34/EÚ ([48])
		— železničné podniky uvedené v článku 3 bode 1 smernice 2012/34/EÚ vrátane prevádzkovateľov servisných zariadení uvedených v článku 3 bode 12 smernice 2012/34/EÚ
	c) Vodná doprava	— spoločnosti prevádzkujúce vnútrozemskú, námornú a pobrežnú osobnú a nákladnú vodnú dopravu uvedené pre námornú dopravu v prílohe I k nariadeniu (ES) č. 725/2004 ([49]), bez jednotlivých plavidiel, ktoré tieto spoločnosti prevádzkujú
		— riadiace orgány prístavov uvedených v článku 3 bode 1 smernice 2005/65/ES ([50]) vrátane ich prístavných zariadení uvedených v článku 2 bode 11 nariadenia (ES) č. 725/2004 a subjekty prevádzkujúce činnosti a zariadenia nachádzajúce sa v prístavoch
		— prevádzkovatelia plavebno-prevádzkových služieb uvedených

[47] 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).

[48] 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).

[49] 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).

[50] 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).

		v článku 3 písm. o) smernice 2002/59/ES ([51])
	d) Cestná doprava	— cestné orgány zodpovedné za kontrolu riadenia cestnej premávky uvedené v článku 2 bode 12 delegovaného nariadenia Komisie (EÚ) 2015/962 ([52]) s **výnimkou verejných subjektov, v prípade ktorých je riadenie dopravy alebo prevádzkovatelia inteligentných dopravných systémov len nepodstatnou súčasťou ich celkovej činnosti.**
		— prevádzkovatelia inteligentných dopravných systémov uvedených v článku 4 bode 1 smernice 2010/40/EÚ ([53])
3. Bankovníctvo		— úverové inštitúcie uvedené v článku 4 bode 1 nariadenia (EÚ) č. 575/2013 ([54]) **[s výnimkou tých, na ktoré sa odkazuje v článku 2 ods. 5 bode 8 smernice 2013/36/EÚ, ktoré sú vyňaté v súlade s článkom 2 ods. 4 nariadenia XX [DORA]]**

[51] 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).

[52] 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).

[53] 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).

[54] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 575/2013 z 26. júna 2013 o prudenciálnych požiadavkách na úverové inštitúcie a investičné spoločnosti a o zmene nariadenia (EÚ) č. 648/2012 (Ú. v. EÚ L 176, 27.6.2013, s. 1).

4. Infraštruktúry finančných trhov		— prevádzkovatelia obchodných miest uvedených v článku 4 bode 24 smernice 2014/65/EÚ ([55])
		— centrálne protistrany (CP) uvedené v článku 2 bode 1 nariadenia (EÚ) č. 648/2012 ([56])
5. Zdravotníctvo		— poskytovatelia zdravotnej starostlivosti uvedení v článku 3 písm. g) smernice 2011/24/EÚ ([57])
		— referenčné laboratóriá EÚ uvedené v článku 15 nariadenia XXXX/XXXX o závažných cezhraničných ohrozeniach zdravia[58]
		— subjekty vykonávajúce činnosti výskumu a vývoja liekov uvedených v článku 1 bode 2 smernice 2001/83/ES ([59]) — Subjekty vyrábajúce základné farmaceutické výrobky a farmaceutické prípravky uvedené v sekcii C divízii 21 NACE Rev. 2 — Subjekty vyrábajúce zdravotnícke pomôcky považované za kritické počas mimoriadnej situácie v oblasti verejného zdravia (ďalej len

[55] 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).

[56] 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).

[57] 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).

[58] [Nariadenie Európskeho parlamentu a Rady o závažných cezhraničných ohrozeniach zdravia a o zrušení rozhodnutia č. 1082/2013/EÚ, odkaz na nariadenie sa aktualizuje po prijatí návrhu dokumentu COM(2020) 727 final].

[59] 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).

		„zoznam pomôcok kritických v mimoriadnej situácii v oblasti verejného zdravia“) uvedené v článku 20 nariadenia XXXX[60]
6. Pitná voda		Dodávatelia a distribútori vody určenej na ľudskú spotrebu uvedenej v článku 2 ods. 1 písm. a) smernice Rady 98/83/ES([61]) s výnimkou distribútorov, pre ktorých je distribúcia vody na ľudskú spotrebu iba **nepodstatnou** časťou 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 a priemyselných odpadových vôd uvedených v článku 2 bodoch 1 až 3 smernice Rady 91/271/EHS ([62]) s **výnimkou podnikov, pre ktoré je zber, likvidácia alebo úprava komunálnych odpadových vôd, odpadových vôd z domácností a priemyselných odpadových vôd len nepodstatnou časťou ich celkovej činnosti.** [...]
8. Digitálna infraštruktúra		— poskytovatelia internetových prepojovacích uzlov
		— poskytovatelia služieb DNS s **výnimkou prevádzkovateľov koreňových menných serverov**

60 Nariadenie Európskeho parlamentu a Rady o posilnenej úlohe Európskej agentúry pre lieky z hľadiska pripravenosti na krízy a krízového riadenia v oblasti liekov a zdravotníckych pomôcok, odkaz na nariadenie sa aktualizuje po prijatí návrhu dokumentu COM(2020) 725 final]

61 Smernica Rady 98/83/ES z 3. novembra 1998 o kvalite vody určenej na ľudskú spotrebu (Ú. v. ES L 330, 5.12.1998, s. 32).

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

		— správcovia mien domény najvyššej úrovne (TLD)
		— poskytovatelia služieb cloud computingu
		— poskytovatelia služieb dátového centra
		— poskytovatelia sietí na sprístupňovanie obsahu
		— poskytovatelia dôveryhodných služieb uvedení v článku 3 bode 19 nariadenia (EÚ) č. 910/2014 ([63])
		— poskytovatelia verejných elektronických komunikačných sietí uvedených v článku 2 bode 8 smernice (EÚ) 2018/1972([64]) alebo poskytovatelia elektronických komunikačných služieb uvedených v článku 2 bode 4 smernice (EÚ) 2018/1972, ktorých služby sú verejne prístupné
8.a Riadenie služieb IKT **(B2B)**		**— Poskytovatelia riadených služieb (MSP)** **— Poskytovatelia riadených bezpečnostných služieb (MSSP)**

63 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).

64 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).

9. **Subjekty** verejnej správy		— Subjekty verejnej správy na úrovni ústrednej štátnej správy**, ako ich vymedzuje členský štát v súlade s vnútroštátnym právom** — [...][65][...] — [...]
10. Kozmický priestor		— Prevádzkovatelia pozemnej infraštruktúry, ktorú vlastnia, spravujú alebo prevádzkujú členské štáty alebo súkromné subjekty, ktorí prispievajú k poskytovaniu vesmírnych služieb, okrem poskytovateľov verejných elektronických komunikačných sietí uvedených v článku 2 bode 8 smernice (EÚ) 2018/1972

[65] [...]

PRÍLOHA II

ODVETVIA, PODODVETVIA A TYPY SUBJEKTOV

Odvetvie	Pododvetvie	Typ subjektu
1. Poštové a kuriérske služby		Poskytovatelia poštových služieb uvedených v článku 2 bode 1[...] smernice 97/67/ES ([66]) **vrátane** [...] poskytovateľov kuriérskych služieb
2. Odpadové hospodárstvo		Podniky vykonávajúce činnosti nakladania s odpadom podľa článku 3 bodu 9 smernice 2008/98/ES ([67]) okrem podnikov, pre ktoré nakladanie s odpadom nepredstavuje hlavnú hospodársku činnosť

[66] 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) **zmenená smernicou Európskeho parlamentu a Rady 2008/6/ES z 20. februára 2008, ktorou sa mení a dopĺňa smernica 97/67/ES s ohľadom na úplné dokončenie vnútorného trhu poštových služieb Spoločenstva (Ú. v. EÚ L 52, 27.2.2008, s. 3)**.

[67] 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).

3. Získavanie, výroba a distribúcia chemických látok		Podniky [...] vyrábajúce a distribuujúce látky a [...] **zmesi** uvedené v článku 3 bodoch ([...]) 9 a 14 nariadenia (ES) č. 1907/2006 ([68]) a **podniky, ktoré z látok alebo zmesí vyrábajú výrobky uvedené v článku 3 bode 3 uvedeného nariadenia.**
4. Výroba, spracovanie a distribúcia potravín		Potravinárske podniky uvedené v článku 3 bode 2 nariadenia (ES) č. 178/2002 ([69])**, 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 uvedené v článku 2 bode 1 nariadenia (EÚ) 2017/745 ([70]) a subjekty vyrábajúce diagnostické zdravotnícke pomôcky in vitro uvedené v článku 2 bode 2 nariadenia (EÚ) 2017/746 ([71]) okrem subjektov vyrábajúcich zdravotnícke pomôcky uvedených v bode 5 prílohy 1.
	b) Výroba počítačových,	Subjekty vykonávajúce akúkoľvek

68 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).

69 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).

70 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).

71 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).

	elektronických a optických výrobkov	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
6. Poskytovatelia digitálnych služieb		— poskytovatelia online trhov
		— poskytovatelia internetových vyhľadávačov
		— poskytovatelia platforiem služieb sociálnej siete