Evropský parlament
2019-2024

Výbor pro občanské svobody, spravedlnost a vnitřní věci

2020/0359(COD)

15.10.2021

STANOVISKO

Výboru pro občanské svobody, spravedlnost a vnitřní věci

pro Výbor pro průmysl, výzkum a energetiku

k návrhu směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Zpravodaj(*): Lukas Mandl(*)

Přidružený výbor – článek 57 jednacího řádu

PA_Legam

STRUČNÉ ODŮVODNĚNÍ

Návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (dále jen „směrnice NIS2“) a o zrušení směrnice (EU) 2016/1148[1] je součástí širšího souboru iniciativ na unijní úrovni zaměřených na zvýšení odolnosti veřejných a soukromých subjektů vůči hrozbám. Cílem návrhu je vyřešit nedostatky stávajících právních předpisů a umožnit subjektům, na něž se vztahuje, lépe reagovat na nové výzvy, které Komise identifikovala ve svém posouzení dopadu, při jehož vypracovávání vedla rozsáhlé konzultace se zúčastněnými stranami. K těmto výzvám patří především zvýšená digitalizace vnitřního trhu a vyvíjející se prostředí bezpečnostních hrozeb.

Právním základem návrhu je článek 114 SFEU, tj. vnitřní trh. Výbor LIBE se nicméně domnívá, že je třeba zdůraznit, že opatření směrnice NIS2 vztahující se k síti a informačním systémům neslouží pouze k zajištění řádného fungování vnitřního trhu. **Směrnice by rovněž měla pomoci přispět k bezpečnosti Unie jako celku**, mimo jiné zabráněním rozdílům v náchylnosti vůči kybernetickým rizikům mezi členskými státy.

Za tímto účelem je třeba **odstranit stávající rozdíly mezi členskými státy** způsobené rozdílným výkladem práva. Zpravodaj proto vítá jednotnou podmínku pro určování subjektů spadajících do působnosti směrnice, kterou nařízení stanoví. Kromě toho předkládá návrhy, jak zabránit rozdílům v provádění: navrhuje uložit Komisi, aby vydala pokyny pro provádění *lex specialis* a kritéria vztahující se na malé a střední podniky (která by rovněž měla zajistit právní jasnost a zabránit zbytečné zátěži), a vyžadovat, aby skupina pro spolupráci dále upřesnila netechnické faktory, které je třeba zohlednit při posuzování rizik dodavatelského řetězce. Dále zdůrazňuje, že spolupráci mezi příslušnými orgány je třeba uskutečňovat jak v rámci členských států, tak i *mezi* nimi, a to v reálném čase.

Návrh zprávy rovněž zohledňuje řadu **doporučení evropského inspektora ochrany údajů**, která učinil ve svém stanovisku ke strategii kybernetické bezpečnosti a směrnici NIS2[2]. V bodech odůvodnění i v normativní části znění se především vyjasňuje, že žádným zpracováním osobních údajů podle směrnice NIS2 není dotčeno nařízení (EU) 2016/679 (GDPR)[3] ani směrnice 2002/58/ES[4] (ochrana soukromí na internetu). Vzhledem k užšímu rozsahu termínu „bezpečnost sítí a informačních systémů“ (vztahuje se pouze na ochranu technologie) ve srovnání s „kybernetickou bezpečností“ (vztahuje se i na činnosti na ochranu uživatelů) je první z uvedených termínů použit pouze v případech, kdy je kontext ryze technický. Co se týče doménových jmen a registračních údajů, navrhuje se ujasnit 1) právní základ zveřejňování „příslušných informací“ pro účely identifikace a kontaktování, 2) kategorie údajů o registraci datové domény, které se zveřejňují (na základě doporučení

[1] 2020/0359(COD).

[2] Stanovisko 5/2021: https://edps.europa.eu/system/files/2021-03/21-03-11_edps_nis2-opinion_en.pdf.

[3] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (text s významem pro EHP), *Úř. věst. L 119, 4.5.2016, s. 1–88*.

[4] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích), *Úř. věst. L 201, 31.7.2002, s. 37–47*.

sdružení ICANN), a 3) subjekty, které mohou představovat „oprávněné žadatele o přístup“. V právním textu je rovněž upřesněno, že návrhem není ovlivněno určování příslušnosti a pravomoci úřadů pro dohled nad ochranou údajů podle GDPR. V neposlední řadě je poskytnut ucelenější právní základ pro spolupráci a výměnu relevantních informací mezi příslušnými úřady v rámci návrhu a dalšími příslušnými orgány dohledu, zejména orgány dohledu podle GDPR.

Další změny návrhu Komise, které zpravodaj výboru LIBE navrhuje, se týkají těchto záležitostí:

- V zájmu zajištění soudržnosti mezi směrnicí NIS2 a navrhovanou směrnicí o odolnosti kritických subjektů[5] byla formulace některých ustanovení sladěna s ustanoveními návrhu této směrnice. V souladu s podobnou změnou plánovanou pro směrnici o odolnosti kritických subjektů, která by se měla týkat stejných odvětví jako směrnice NIS2, se navrhuje zařadit do její působnosti „výrobu, zpracování a distribuci potravin“.
- Pokud jde o osobní údaje, vyjasňuje se, že vyhledávání sítí a informačních systémů týmy CSIRT by nemělo být pouze v souladu s nařízením (EU) 2016/679 (GDPR)[6], ale i se směrnicí 2002/58/ES[7] (ochrana soukromí na internetu). Mezinárodní předávání osobních údajů podle této směrnice by mělo být v souladu s kapitolou V nařízení GDPR.
- Skupina pro spolupráci by se měla scházet dvakrát spíše než jen jednou v roce, aby posoudila nejnovější vývoj v oblasti kybernetické bezpečnosti. Schůzí skupiny pro spolupráci by se měl jako pozorovatel účastnit Evropský sbor pro ochranu osobních údajů.
- Agentura ENISA by měla vydávat zprávy o stavu kybernetické bezpečnosti v Unii každý rok spíše než jednou za dva roky. Zpráva by měla zohlednit také dopad kybernetických bezpečnostních incidentů na ochranu osobních údajů v Unii.
- Lhůta pro oznamování incidentů je sladěna s lhůtou pro oznamování případů porušení pravidel podle nařízení GDPR a činí tedy 72 hodin.
- Zatímco oznamování skutečných kybernetických bezpečnostních incidentů základními a důležitými subjekty by mělo být vskutku povinné, oznamování kybernetických hrozeb by mělo být dobrovolné, aby se snížila administrativní zátěž a zabránilo nadměrnému množství zpráv. Aby byl incident považován za významný, měl by způsobit skutečnou škodu a mít dopad na další fyzické a právnické osoby, místo toho, aby byla tato škoda či dopad „možný“.
- Okolnosti, které je třeba zohlednit při rozhodování o sankci za porušení pravidel pro kybernetickou bezpečnost, jsou sladěny s nařízením GDPR. Nemělo by být možné uložit fyzickým osobám dočasný zákaz výkonu řídících funkcí, protože by to bylo v rozporu se stávající praxí týkající se odpovědnosti podle práva Unie.

[5] 2020/0365(COD).

[6] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (text s významem pro EHP), *Úř. věst. L 119, 4.5.2016, s. 1–88*.

[7] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích), *Úř. věst. L 201, 31.7.2002, s. 37–47*.

• Aby se zabránilo poškození pověsti, subjekty by neměly mít povinnost zveřejňovat aspekty nedodržení požadavků podle této směrnice ani totožnost fyzických nebo právnických osob, které se tohoto porušení dopustily.

POZMĚŇOVACÍ NÁVRHY

Výbor pro občanské svobody, spravedlnost a vnitřní věci vyzývá Výbor pro průmysl, výzkum a energetiku jako příslušný výbor, aby zohlednil tyto pozměňovací návrhy:

Pozměňovací návrh 1

Návrh směrnice
Bod odůvodnění 1

Znění navržené Komisí	*Pozměňovací návrh*
(1) Cílem směrnice Evropského parlamentu a Rady (EU) 2016/1148[11] bylo budovat schopnosti v oblasti kybernetické bezpečnosti v Unii, zmírňovat hrozby pro sítě a informační systémy užívané k poskytování základních služeb v klíčových odvětvích a zajišťovat kontinuitu takových služeb v případě kybernetických bezpečnostních incidentů, a přispívat tak k účinnému fungování hospodářství a společnosti v Unii.	(1) Cílem směrnice Evropského parlamentu a Rady (EU) 2016/1148[11] bylo budovat schopnosti v oblasti kybernetické bezpečnosti v Unii, zmírňovat hrozby pro sítě a informační systémy užívané k poskytování základních služeb v klíčových odvětvích a zajišťovat kontinuitu takových služeb v případě kybernetických bezpečnostních incidentů, a přispívat tak k ***bezpečnosti a*** účinnému fungování hospodářství a společnosti v Unii.
[11] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Úř. věst. L 194/1, 19.7.2016, s. 1). 1).	[11] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Úř. věst. L 194/1, 19.7.2016, s. 1). 1).

Pozměňovací návrh 2

Návrh směrnice
Bod odůvodnění 2

Znění navržené Komisí	*Pozměňovací návrh*
(2) Od vstupu směrnice (EU) 2016/1148 v platnost bylo ve zvyšování úrovně odolnosti Unie v oblasti	(2) Od vstupu směrnice (EU) 2016/1148 v platnost bylo ve zvyšování úrovně odolnosti Unie v oblasti

kybernetické bezpečnosti dosaženo významného pokroku. Z přezkumu uvedené směrnice vyplynulo, že posloužila jako katalyzátor institucionálního a regulačního přístupu ke kybernetické bezpečnosti v Unii, a současně připravila půdu pro významnou změnu v myšlení. Uvedená směrnice zajistila dokončení vnitrostátních rámců stanovením národních strategií kybernetické bezpečnosti, stanovením vnitrostátních schopností a prováděním regulačních opatření pokrývajících základní infrastruktury a subjekty určené každým členským státem. Přispěla rovněž ke spolupráci na úrovni Unie vytvořením skupiny pro spolupráci***12*** a sítě vnitrostátních bezpečnostních týmů typu CSIRT (dále jen „síť CSIRT“)***13***. I přes tyto úspěchy odhalil přezkum směrnice (EU) 2016/1148 přirozené nedostatky, které jí brání v účinném řešení současných a vznikajících výzev v oblasti kybernetické bezpečnosti.

kybernetické bezpečnosti dosaženo významného pokroku. Z přezkumu uvedené směrnice vyplynulo, že posloužila jako katalyzátor institucionálního a regulačního přístupu ke kybernetické bezpečnosti v Unii, a současně připravila půdu pro významnou změnu v myšlení. Uvedená směrnice zajistila dokončení vnitrostátních rámců stanovením národních strategií kybernetické bezpečnosti, stanovením vnitrostátních schopností a prováděním regulačních opatření pokrývajících základní infrastruktury a subjekty určené každým členským státem. Přispěla rovněž ke spolupráci na úrovni Unie vytvořením skupiny pro spolupráci a sítě vnitrostátních bezpečnostních týmů typu CSIRT (dále jen „síť CSIRT“). I přes tyto úspěchy odhalil přezkum směrnice (EU) 2016/1148 přirozené nedostatky, které jí brání v účinném řešení současných a vznikajících výzev v oblasti kybernetické bezpečnosti. ***Rozšíření on-line činností v souvislosti s pandemií COVID-19 navíc upozornilo na význam kybernetické bezpečnosti, která je nezbytná pro to, aby občané EU mohli důvěřovat inovacím a konektivitě, jakož i na význam rozsáhlého vzdělávání a odborné přípravy v této oblasti. Komise by proto měla podporovat členské státy při tvorbě vzdělávacích programů v oblasti kybernetické bezpečnosti s cílem umožnit důležitým a základním subjektům přijímat odborníky v oblasti kybernetické bezpečnosti, kteří jim umožní splnit povinnosti vyplývající z této směrnice.***

---

[12] Článek 11 směrnice (EU) 2016/1148.

[13] Článek 12 směrnice (EU) 2016/1148.

[12] Článek 11 směrnice (EU) 2016/1148.

[13] Článek 12 směrnice (EU) 2016/1148.

Pozměňovací návrh 3

Návrh směrnice
Bod odůvodnění 3

Znění navržené Komisí	*Pozměňovací návrh*
(3) Sítě a informační systémy se rozvinuly v ústřední prvek každodenního života s rychlou digitální transformací a vzájemnou propojeností společnosti, včetně přeshraniční výměny. Tento vývoj vedl k prudkému rozšíření prostředí kybernetických bezpečnostních hrozeb a přináší nové výzvy, které vyžadují přizpůsobené, koordinované a inovativní reakce ve všech členských státech. Počet, rozsah, sofistikovanost, četnost výskytu a dopad kybernetických bezpečnostních incidentů narůstají a představují značnou hrozbu pro fungování sítí a informačních systémů. V důsledku toho mohou kybernetické incidenty brzdit provádění hospodářských činností na vnitřním trhu, způsobovat finanční ztráty, narušovat důvěru uživatelů a způsobovat velké škody hospodářství a ***společnosti Unie***. Připravenost a účinnost v oblasti kybernetické bezpečnosti ***jsou dnes proto pro*** řádné fungování vnitřního trhu důležitější než kdy předtím.	(3) Sítě a informační systémy se rozvinuly v ústřední prvek každodenního života s rychlou digitální transformací a vzájemnou propojeností společnosti, včetně přeshraniční výměny. Tento vývoj vedl k prudkému rozšíření prostředí kybernetických bezpečnostních hrozeb a přináší nové výzvy, které vyžadují přizpůsobené, koordinované a inovativní reakce ve všech členských státech. Počet, rozsah, sofistikovanost, četnost výskytu a dopad kybernetických bezpečnostních incidentů narůstají a představují značnou hrozbu pro fungování sítí a informačních systémů. V důsledku toho mohou kybernetické incidenty brzdit provádění hospodářských činností na vnitřním trhu, způsobovat finanční ztráty, narušovat důvěru uživatelů a způsobovat velké škody hospodářství ***Unie, fungování naší demokracie*** a ***hodnotám a svobodě, na kterých je naše společnost založena***. ***S ohledem na digitální transformaci každodenních činnosti v celé Unii jsou dnes proto*** připravenost a účinnost v oblasti kybernetické bezpečnosti ***pro bezpečnost Unie a*** řádné fungování vnitřního trhu důležitější než kdy předtím. ***To vyžaduje užší spolupráci orgánů jak v rámci členských států, tak mezi nimi, jakož i mezi vnitrostátními orgány a odpovědnými institucemi Unie.***

Pozměňovací návrh 4

Návrh směrnice
Bod odůvodnění 5

Znění navržené Komisí	*Pozměňovací návrh*
(5) Všechny tyto rozdíly vyvolávají roztříštěnost vnitřního trhu a mohou mít škodlivý účinek na jeho fungování s tím, že ovlivňují zejména přeshraniční poskytování služeb a úroveň odolnosti	(5) Všechny tyto rozdíly vyvolávají roztříštěnost vnitřního trhu a mohou mít škodlivý účinek na jeho fungování s tím, že ovlivňují zejména přeshraniční poskytování služeb a úroveň odolnosti

v oblasti kybernetické bezpečnosti v důsledku uplatňování odlišných norem. Cílem této směrnice je takové značné rozdíly mezi členskými státy odstranit, zejména stanovením minimálních pravidel upravujících fungování koordinovaného regulačního rámce, stanovením mechanismů účinné spolupráce příslušných orgánů v každém členském státě, aktualizací seznamu odvětví a činností, na něž se vztahují povinnosti v oblasti kybernetické bezpečnosti, a zavedením účinných nápravných opatření a sankcí, jež napomáhají účinnému vymáhání těchto povinností. Směrnice (EU) 2016/1148 by proto měla být zrušena a nahrazena touto směrnicí.

v oblasti kybernetické bezpečnosti v důsledku uplatňování odlišných norem. ***Tyto rozdíly mohou v konečném důsledku vést k větší zranitelnosti některých členských států vůči hrozbám v oblasti kybernetické bezpečnosti, což může mít dopad na celou Unii, jak pokud jde o vnitřní trh, tak o její celkovou bezpečnost.*** Cílem této směrnice je takové značné rozdíly mezi členskými státy odstranit, zejména stanovením minimálních pravidel upravujících fungování koordinovaného regulačního rámce, stanovením mechanismů účinné spolupráce příslušných orgánů v každém členském státě ***a mezi příslušnými orgány členských států, jež bude probíhat v reálném čase***, aktualizací seznamu odvětví a činností, na něž se vztahují povinnosti v oblasti kybernetické bezpečnosti, a zavedením účinných nápravných opatření a sankcí, jež napomáhají účinnému vymáhání těchto povinností. Směrnice (EU) 2016/1148 by proto měla být zrušena a nahrazena touto směrnicí.

Pozměňovací návrh 5

Návrh směrnice
Bod odůvodnění 6

Znění navržené Komisí	*Pozměňovací návrh*
(6) Tato směrnice ponechává nedotčenou schopnost členských států přijímat nezbytná opatření, aby zajistily ochranu svých základních ***bezpečnostních zájmů***, ochranu veřejného pořádku a veřejné bezpečnosti a umožnily vyšetřování, odhalování a stíhání trestných činů v souladu s právem Unie. V souladu s článkem 346 SFEU není žádný členský stát povinen poskytovat informace, jejichž zpřístupnění by bylo v rozporu se základními zájmy jeho veřejné bezpečnosti. V tomto ohledu jsou relevantní pravidla členských států a Unie o ochraně utajovaných informací, dohody o	(6) Tato směrnice ponechává nedotčenou schopnost členských států přijímat nezbytná opatření, aby zajistily ochranu svých základních ***zájmů v oblasti národní bezpečnosti***, ochranu veřejného pořádku a veřejné bezpečnosti a umožnily ***prevenci,*** vyšetřování, odhalování a stíhání trestných činů v souladu s právem Unie. V souladu s článkem 346 SFEU není žádný členský stát povinen poskytovat informace, jejichž zpřístupnění by bylo v rozporu se základními zájmy jeho veřejné bezpečnosti. V tomto ohledu jsou relevantní pravidla členských států a Unie o ochraně utajovaných informací, dohody o

zachování důvěrnosti údajů nebo neformální dohody o zachování důvěrnosti, jako je například tzv. „semaforový protokol“ (Traffic Light Protocol)[14] .

[14] Semaforový protokol je prostředek pro toho, kdo sdílí informace, aby informoval své publikum o jakýchkoli omezeních dalšího šíření těchto informací. Používá se téměř ve všech komunitách CSIRT a některých střediscích pro sdílení a analýzu informací (ISAC).

zachování důvěrnosti údajů nebo neformální dohody o zachování důvěrnosti, jako je například tzv. „semaforový protokol“ (Traffic Light Protocol)[14].

[14] Semaforový protokol je prostředek pro toho, kdo sdílí informace, aby informoval své publikum o jakýchkoli omezeních dalšího šíření těchto informací. Používá se téměř ve všech komunitách CSIRT a některých střediscích pro sdílení a analýzu informací (ISAC).

Pozměňovací návrh 6

Návrh směrnice
Bod odůvodnění 8

Znění navržené Komisí	*Pozměňovací návrh*
(8) ***V*** souladu se směrnicí (EU) 2016/1148 byly ***členské státy*** odpovědné za určení toho, které subjekty splňují kritéria pro zařazení mezi provozovatele základních služeb (dále jen „proces určování“)***. S cílem odstranit značné rozdíly*** mezi členskými státy v tomto ohledu ***a zajistit právní jistotu pro všechny příslušné subjekty, pokud jde o požadavky na řízení rizik a povinnosti hlášení***, by ***mělo*** být stanoveno jednotné kritérium, které určí subjekty, jež spadají do oblasti působnosti této směrnice. Toto kritérium by mělo spočívat v uplatnění pravidla velikostního omezení, podle kterého by do oblasti působnosti této směrnice spadaly všechny střední a velké podniky ve smyslu doporučení Komise 2003/361/ES[15], které působí v odvětvích nebo poskytují druh služeb, na něž se vztahuje tato směrnice. Od členských států by nemělo být vyžadováno, aby stanovily seznam subjektů, které splňují toto obecně použitelné kritérium související s velikostí podniku.	(8) ***Odpovědnost členských států – neboť v*** souladu se směrnicí (EU) 2016/1148 byly odpovědné za určení toho, které subjekty splňují kritéria pro zařazení mezi provozovatele základních služeb (dále jen „proces určování“)***, – vedla ke značným rozdílům*** mezi členskými státy v tomto ohledu***. Aniž by byly dotčeny konkrétní výjimky v této směrnici***, ***mělo*** by být stanoveno jednotné kritérium, které určí subjekty, jež spadají do oblasti působnosti této směrnice***, a to s cílem odstranit tyto rozdíly a zajistit právní jistotu, pokud jde o požadavky na řízení rizik a povinnosti hlášení pro všechny příslušné subjekty***. Toto kritérium by mělo spočívat v uplatnění pravidla velikostního omezení, podle kterého by do oblasti působnosti této směrnice spadaly všechny střední a velké podniky ve smyslu doporučení Komise 2003/361/ES[15], které působí v odvětvích nebo poskytují druh služeb, na něž se vztahuje tato směrnice. Od členských států by nemělo být vyžadováno, aby stanovily seznam subjektů, které splňují toto obecně použitelné kritérium související s velikostí

podniku.

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

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

Pozměňovací návrh 7

Návrh směrnice
Bod odůvodnění 8 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(8a) S ohledem na rozdíly ve vnitrostátních rámcích veřejné správy si členské státy ponechávají svou rozhodovací pravomoc, pokud jde o určení subjektů, které spadají do oblasti působnosti této směrnice.

Pozměňovací návrh 8

Návrh směrnice
Bod odůvodnění 9

Znění navržené Komisí	*Pozměňovací návrh*
(9) Tato směrnice by se ***však*** měla vztahovat i na malé subjekty nebo mikrosubjekty, které splňují určitá kritéria, jež naznačují klíčovou úlohu pro hospodářství nebo společnosti členských států nebo pro konkrétní odvětví či konkrétní druhy služeb. Členské státy by měly být odpovědné za stanovení seznamu takových subjektů a předložit ho Komisi.	(9) Tato směrnice by se měla vztahovat i na malé subjekty nebo mikrosubjekty, které splňují určitá kritéria, jež naznačují klíčovou úlohu pro hospodářství nebo společnosti členských států nebo pro konkrétní odvětví či konkrétní druhy služeb ***na základě posouzení rizik, a to včetně subjektů definovaných jako kritické subjekty nebo jako subjekty rovnocenné kritickým subjektům podle směrnice Evropského parlamentu a Rady (EU) XXX/XXX[1a]***. Členské státy by měly být odpovědné za stanovení seznamu takových subjektů a předložit ho Komisi.
	[1a] Směrnice Evropského parlamentu a Rady (EU) [XXX/XXX] ze dne XXX o

odolnosti kritických subjektů (Úř. věst…).

Pozměňovací návrh 9

Návrh směrnice
Bod odůvodnění 10

Znění navržené Komisí	*Pozměňovací návrh*
(10) Komise ***může*** ve spolupráci se skupinou pro spolupráci vydávat pokyny ohledně plnění kritérií platných pro mikropodniky a malé ***podniky***.	(10) Komise ***by*** ve spolupráci se skupinou pro spolupráci ***měla*** vydávat pokyny ohledně plnění kritérií platných pro mikropodniky a malé ***subjekty***.

Pozměňovací návrh 10

Návrh směrnice
Bod odůvodnění 12

Znění navržené Komisí	*Pozměňovací návrh*
(12) Právní předpisy a nástroje specifické pro jednotlivá odvětví mohou přispět k zajištění vysoké úrovně kybernetické bezpečnosti při současném plném zohlednění zvláštností a složitosti těchto odvětví. Pokud právní akt Unie specifický pro určité odvětví vyžaduje, aby základní nebo důležité subjekty přijaly opatření k řízení kybernetických bezpečnostních rizik, nebo aby oznamovaly incidenty nebo závažné kybernetické hrozby s alespoň rovnocenným účinkem jako povinnosti stanovené v této směrnici, měla by platit tato ustanovení specifická pro dané odvětví, včetně ustanovení o dohledu a vymáhání. Komise ***může*** vydávat pokyny v souvislosti s prováděním lex specialis. Tato směrnice nebrání přijetí dalších aktů Unie specifických pro určitá odvětví a týkajících se opatření k řízení kybernetických bezpečnostních rizik a oznamování incidentů. Touto směrnicí nejsou dotčeny stávající prováděcí pravomoci, jež byly Komisi svěřeny v řadě odvětví, včetně odvětví dopravy a	(12) Právní předpisy a nástroje specifické pro jednotlivá odvětví mohou přispět k zajištění vysoké úrovně kybernetické bezpečnosti při současném plném zohlednění zvláštností a složitosti těchto odvětví. Pokud právní akt Unie specifický pro určité odvětví vyžaduje, aby základní nebo důležité subjekty přijaly opatření k řízení kybernetických bezpečnostních rizik, nebo aby oznamovaly incidenty nebo závažné kybernetické hrozby s alespoň rovnocenným účinkem jako povinnosti stanovené v této směrnici, měla by platit tato ustanovení specifická pro dané odvětví, včetně ustanovení o dohledu a vymáhání. Komise ***by měla*** vydávat pokyny v souvislosti s prováděním lex specialis. Tato směrnice nebrání přijetí dalších aktů Unie specifických pro určitá odvětví a týkajících se opatření k řízení kybernetických bezpečnostních rizik a oznamování incidentů. Touto směrnicí nejsou dotčeny stávající prováděcí pravomoci, jež byly Komisi svěřeny v řadě odvětví, včetně odvětví dopravy a

energetiky.

energetiky.

Pozměňovací návrh 11

Návrh směrnice
Bod odůvodnění 14

Znění navržené Komisí	*Pozměňovací návrh*
(14) Vzhledem ke vzájemným vazbám mezi kybernetickou bezpečností a fyzickou bezpečností subjektů by měl být zajištěn soudržný přístup ke směrnici Evropského parlamentu a Rady (EU) XXX/XXX[17] a k této směrnici. Za tímto účelem by členské státy měly zajistit, aby klíčové subjekty a rovnocenné subjekty podle směrnice (EU) XXX/XXX byly považovány za základní subjekty podle této směrnice. Členské státy by také měly zajistit, aby jejich strategie kybernetické bezpečnosti stanovily rámec politik pro posílení koordinace mezi ***příslušným orgánem*** podle této směrnice a ***příslušným orgánem*** podle směrnice (EU) XXX/XXX v souvislosti se sdílením informací o incidentech a kybernetických hrozbách a plněním úkolů v oblasti dohledu. Orgány by podle obou směrnic měly spolupracovat a vyměňovat si informace, zejména informace týkající se určení klíčových subjektů, kybernetických hrozeb, kybernetických bezpečnostních rizik, incidentů dotýkajících se klíčových subjektů a opatření v oblasti kybernetické bezpečnosti přijatých ***klíčovými*** subjekty. Příslušným orgánům podle této směrnice by mělo být umožněno, aby na žádost příslušných orgánů podle směrnice (EU) XXX/XXX ***vykonávaly své dohledové a vymáhací pravomoci vůči*** subjektu, který byl označen jako klíčový. Oba orgány by za tímto účelem měly spolupracovat a vyměňovat si informace.	(14) Vzhledem ke vzájemným vazbám mezi kybernetickou bezpečností a fyzickou bezpečností subjektů by měl být zajištěn soudržný přístup ke směrnici Evropského parlamentu a Rady (EU) XXX/XXX[17] a k této směrnici***, kdykoli to bude možné a vhodné***. Za tímto účelem by členské státy měly zajistit, aby klíčové subjekty a rovnocenné subjekty podle směrnice (EU) XXX/XXX byly považovány za základní subjekty podle této směrnice. Členské státy by také měly zajistit, aby jejich strategie kybernetické bezpečnosti stanovily rámec politik pro posílení koordinace mezi ***orgány v rámci členských států a mezi členskými státy, jež jsou příslušné*** podle této směrnice a podle směrnice (EU) XXX/XXX***,*** v souvislosti se sdílením informací o ***kybernetických*** incidentech a kybernetických hrozbách a plněním úkolů v oblasti dohledu. Orgány by podle obou směrnic měly spolupracovat***, a to v rámci členských států i mezi členskými státy,*** a vyměňovat si informace, zejména informace týkající se určení klíčových subjektů, kybernetických hrozeb, kybernetických bezpečnostních rizik, incidentů dotýkajících se klíčových subjektů a opatření v oblasti kybernetické bezpečnosti přijatých ***příslušnými orgány podle této směrnice, jež jsou relevantní pro klíčové*** subjekty. Příslušným orgánům podle této směrnice by mělo být umožněno, aby na žádost příslušných orgánů podle směrnice (EU) XXX/XXX ***posoudily kybernetickou bezpečnost základního*** subjektu, který byl označen jako klíčový. Oba orgány by za tímto účelem měly spolupracovat a vyměňovat si

informace ***v reálném čase***.

[17][vložte úplný název a údaje o vyhlášení v Úředním věstníku, až budou známy]

[17][vložte úplný název a údaje o vyhlášení v Úředním věstníku, až budou známy]

Pozměňovací návrh 12

Návrh směrnice
Bod odůvodnění 18

Znění navržené Komisí	*Pozměňovací návrh*
(18) Služby, jež nabízejí poskytovatelé služeb datových center, nemusí být vždy poskytovány ve formě služeb cloud computingu. Datová centra tedy ne vždy tvoří součást infrastruktury cloud computingu. Aby bylo možné řídit všechna rizika pro ***bezpečnost sítí a informačních systémů***, měla by se tato směrnice vztahovat také na poskytovatele takových služeb datových center, které nejsou službami cloud computingu. Pro účely této směrnice by pojem „služba datových center“ měl zahrnovat poskytování služby, která zahrnuje struktury nebo skupiny struktur určené pro centralizované úpravy, vzájemné propojení a provozování informačních technologií a síťových zařízení poskytujících služby ukládání, zpracování a přepravu dat spolu se všemi zařízeními a infrastrukturami pro rozvod energie a kontrolu životního prostředí. Pojem „služba datových center“ se nevztahuje na interní, firemní datová centra vlastněná a provozovaná pro vlastní potřebu dotyčného subjektu.	(18) Služby, jež nabízejí poskytovatelé služeb datových center, nemusí být vždy poskytovány ve formě služeb cloud computingu. Datová centra tedy ne vždy tvoří součást infrastruktury cloud computingu. Aby bylo možné řídit všechna rizika pro ***kybernetickou bezpečnost***, měla by se tato směrnice vztahovat také na poskytovatele takových služeb datových center, které nejsou službami cloud computingu. Pro účely této směrnice by pojem „služba datových center“ měl zahrnovat poskytování služby, která zahrnuje struktury nebo skupiny struktur určené pro centralizované úpravy, vzájemné propojení a provozování informačních technologií a síťových zařízení poskytujících služby ukládání, zpracování a přepravu dat spolu se všemi zařízeními a infrastrukturami pro rozvod energie a kontrolu životního prostředí. Pojem „služba datových center“ se nevztahuje na interní, firemní datová centra vlastněná a provozovaná pro vlastní potřebu dotyčného subjektu.

Pozměňovací návrh 13

Návrh směrnice
Bod odůvodnění 20

Znění navržené Komisí	*Pozměňovací návrh*
(20) Tyto rostoucí vzájemné závislosti	(20) Tyto rostoucí vzájemné závislosti

jsou výsledkem stále více přeshraniční a vzájemně propojené sítě poskytování služeb pomocí klíčových infrastruktur v celé Unii v odvětvích energetiky, dopravy, digitální infrastruktury, pitné a odpadní vody, zdravotnictví, některých prvků veřejné správy a rovněž vesmíru, pokud jde o poskytování určitých služeb závisejících na pozemních infrastrukturách, které vlastní, řídí a provozují buď členské státy, nebo soukromé subjekty, a proto nezahrnují infrastruktury vlastněné, řízené a provozované Unií nebo jménem Unie v rámci jejích vesmírných programů. Tyto vzájemné závislosti znamenají, že jakékoli narušení hospodářské soutěže, a dokonce i takové narušení, které je původně omezeno na jeden subjekt nebo jedno odvětví, může mít širší dominové účinky, jež mohou potenciálně mít dalekosáhlé negativní dopady na poskytování služeb na celém vnitřním trhu. Pandemie COVID-19 ***prokázala*** zranitelnost našich stále více vzájemně závislých společností, jsou-li vystaveny málo pravděpodobným rizikům.	jsou výsledkem stále více přeshraniční a vzájemně propojené sítě poskytování služeb pomocí klíčových infrastruktur v celé Unii v odvětvích energetiky, dopravy, digitální infrastruktury, pitné a odpadní vody, ***produkce, zpracování a distribuce potravin,*** zdravotnictví, některých prvků veřejné správy a rovněž vesmíru, pokud jde o poskytování určitých služeb závisejících na pozemních infrastrukturách, které vlastní, řídí a provozují buď členské státy, nebo soukromé subjekty, a proto nezahrnují infrastruktury vlastněné, řízené a provozované Unií nebo jménem Unie v rámci jejích vesmírných programů. Tyto vzájemné závislosti znamenají, že jakékoli narušení hospodářské soutěže, a dokonce i takové narušení, které je původně omezeno na jeden subjekt nebo jedno odvětví, může mít širší dominové účinky, jež mohou potenciálně mít dalekosáhlé negativní dopady na poskytování služeb na celém vnitřním trhu. ***Vystupňované útoky na informační systémy během*** pandemie COVID-19 ***prokázaly*** zranitelnost našich stále více vzájemně závislých společností, jsou-li vystaveny málo pravděpodobným rizikům. ***Proto jsou nutné další investice do kybernetické bezpečnosti.***

Pozměňovací návrh 14

Návrh směrnice
Bod odůvodnění 20 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(20a) Je klíčové zvýšit informovanost o kybernetické bezpečnosti a kybernetickou odolnost ve všech kritických a důležitých subjektech, včetně subjektů veřejné správy.

Pozměňovací návrh 15

Návrh směrnice
Bod odůvodnění 21

Znění navržené Komisí	*Pozměňovací návrh*
(21) Vzhledem k odlišnostem jednotlivých vnitrostátních správních struktur a s cílem podpořit již existující odvětvová opatření nebo kontrolní a regulační orgány Unie by členské státy měly mít možnost určit více než jeden vnitrostátní příslušný orgán odpovědný za plnění úkolů spojených s bezpečností sítí a informačních systémů základních a důležitých subjektů podle této směrnice. Členským státům by mělo být umožněno, aby tuto úlohu svěřily již existujícímu orgánu.	(21) Vzhledem k odlišnostem jednotlivých vnitrostátních správních struktur a s cílem podpořit již existující odvětvová opatření nebo kontrolní a regulační orgány Unie by členské státy měly mít možnost určit více než jeden vnitrostátní příslušný orgán odpovědný za plnění úkolů spojených s bezpečností sítí a informačních systémů základních a důležitých subjektů podle této směrnice. Členským státům by mělo být umožněno, aby tuto úlohu svěřily již existujícímu orgánu***, a měly by zajistit, aby tento orgán měl odpovídající zdroje pro účinné a efektivní plnění svých úkolů***.

Pozměňovací návrh 16

Návrh směrnice
Bod odůvodnění 22

Znění navržené Komisí	*Pozměňovací návrh*
(22) Pro usnadnění přeshraniční spolupráce a komunikace mezi orgány a za účelem účinného provedení této směrnice je nezbytné, aby každý členský stát určil na vnitrostátní úrovni jednotné kontaktní místo pověřené koordinací v oblasti ***bezpečnosti sítí a informačních systémů*** a přeshraniční spolupráce na úrovni Unie.	(22) Pro usnadnění přeshraniční spolupráce a komunikace mezi orgány a za účelem účinného provedení této směrnice je nezbytné, aby každý členský stát určil na vnitrostátní úrovni jednotné kontaktní místo pověřené koordinací v oblasti ***kybernetické bezpečnosti*** a přeshraniční spolupráce na úrovni Unie.

Pozměňovací návrh 17

Návrh směrnice
Bod odůvodnění 23

Znění navržené Komisí	*Pozměňovací návrh*
(23) Příslušné orgány nebo týmy CSIRT	(23) Příslušné orgány nebo týmy CSIRT

by měly od subjektů dostávat oznámení o incidentech účinným a efektivním způsobem. Jednotným kontaktním místům by mělo být uloženo, aby zasílala oznámení o incidentech jednotným kontaktním místům ***jiných dotčených*** členských států. Aby bylo zajištěno jedno jednotné kontaktní místo v každém členském státě, měly by být jednotným kontaktním místům na úrovni členských států zasílány příslušné informace o incidentech týkajících se subjektů ve finančním odvětví od příslušných orgánů podle nařízení XXXX/XXXX, které by tato kontaktní místa měla být podle této směrnice schopna případně zasílat příslušným vnitrostátním orgánům nebo týmům CSIRT.

by měly od subjektů dostávat oznámení o incidentech účinným a efektivním způsobem. Jednotným kontaktním místům by mělo být uloženo, aby ***v reálném čase*** zasílala oznámení o incidentech jednotným kontaktním místům ***všech ostatních*** členských států. Aby bylo zajištěno jedno jednotné kontaktní místo v každém členském státě, měly by být jednotným kontaktním místům na úrovni členských států zasílány příslušné informace o incidentech týkajících se subjektů ve finančním odvětví od příslušných orgánů podle nařízení XXXX/XXXX, které by tato kontaktní místa měla být podle této směrnice schopna případně zasílat příslušným vnitrostátním orgánům nebo týmům CSIRT.

Pozměňovací návrh 18

Návrh směrnice
Bod odůvodnění 25

Znění navržené Komisí	*Pozměňovací návrh*
(25) Pokud jde o osobní údaje, týmům CSIRT by mělo být umožněno, aby v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679[19] jménem a na žádost subjektu podle této směrnice ***aktivně prohledávaly sítě*** a ***informační systémy***, které používá k poskytování svých služeb. Členské státy by se měly zaměřit na to, aby všem odvětvovým týmům CSIRT zajistily stejné technické podmínky. Při budování vnitrostátních týmů CSIRT mohou členské státy požádat o součinnost Agenturu Evropské unie pro kybernetickou bezpečnost (ENISA).	(25) Pokud jde o osobní údaje, týmům CSIRT by mělo být umožněno, aby v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/67919 ***a směrnicí 2002/58/ES*** jménem a na žádost subjektu podle této směrnice ***prováděly bezpečnostní kontrolu informačních systémů*** a ***rozsahu sítě***, které používá k poskytování svých služeb***, s cílem odhalit konkrétní hrozby, zmírnit je nebo jim zabránit***. Členské státy by se měly zaměřit na to, aby všem odvětvovým týmům CSIRT zajistily stejné technické podmínky. Při budování vnitrostátních týmů CSIRT mohou členské státy požádat o součinnost Agenturu Evropské unie pro kybernetickou bezpečnost (ENISA). ***Kromě toho by rizika v oblasti kybernetické bezpečnosti neměla být nikdy využívána jako záminka pro porušování základních práv.***

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

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

Pozměňovací návrh 19

Návrh směrnice
Bod odůvodnění 27

Znění navržené Komisí	*Pozměňovací návrh*
(27) V souladu s přílohou doporučení Komise (EU) 2017/1548 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize (dále jen „plán“)[20] by rozsáhlý incident měl označovat incident s významným dopadem na nejméně dva členské státy nebo takový incident, při kterém narušení přesahuje schopnost členského státu na něj reagovat. V závislosti na jejich příčině a dopadu mohou rozsáhlé incidenty eskalovat a přejít ve skutečné krize, jež neumožní řádné fungování vnitřního trhu. Vzhledem k širokému dopadu a ve většině případů i přeshraniční povaze takových incidentů by členské státy a příslušné orgány, instituce a agentury Unie měly na technické, operativní a politické úrovni spolupracovat a odpovídajícím způsobem koordinovat reakci v celé Unii.	(27) V souladu s přílohou doporučení Komise (EU) 2017/1548 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize (dále jen „plán“)[20] by rozsáhlý incident měl označovat incident s významným dopadem na nejméně dva členské státy nebo takový incident, při kterém narušení přesahuje schopnost členského státu na něj reagovat. V závislosti na jejich příčině a dopadu mohou rozsáhlé incidenty eskalovat a přejít ve skutečné krize, jež neumožní řádné fungování vnitřního trhu ***nebo představují vážná rizika pro veřejnou bezpečnost v několika členských státech nebo v Unii jako celku***. Vzhledem k širokému dopadu a ve většině případů i přeshraniční povaze takových incidentů by členské státy a příslušné orgány, instituce a agentury Unie měly na technické, operativní a politické úrovni spolupracovat a odpovídajícím způsobem koordinovat reakci v celé Unii. ***Členské státy by měly sledovat způsob, jakým jsou prováděna pravidla EU, vzájemně se podporovat v případě jakýchkoli přeshraničních problémů, navázat strukturovanější dialog se soukromým sektorem a spolupracovat v oblasti bezpečnostních rizik a hrozeb spojených s novými technologiemi, jako tomu bylo v případě technologie 5G.***

[20] Doporučení Komise (EU) 2017/1584 ze dne 13. září 2017 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize (Úř. věst. L 239, 19.9.2017, s. 36).

[20] Doporučení Komise (EU) 2017/1584 ze dne 13. září 2017 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize (Úř. věst. L 239, 19.9.2017, s. 36).

Pozměňovací návrh 20

Návrh směrnice
Bod odůvodnění 33

Znění navržené Komisí	*Pozměňovací návrh*
(33) Při vypracování pokynů by skupina pro spolupráci měla důsledně: mapovat vnitrostátní řešení a zkušenosti, posuzovat dopad výstupů skupiny pro spolupráci na ***přístupy členských států***, diskutovat o problémech spojených s prováděním a formulovat konkrétní doporučení, která je třeba zohlednit prostřednictvím lepšího provádění stávajících pravidel.	(33) Při vypracování pokynů by skupina pro spolupráci měla důsledně: mapovat vnitrostátní ***a odvětvová*** řešení a zkušenosti, posuzovat dopad výstupů skupiny pro spolupráci na ***vnitrostátní a odvětvové přístupy***, diskutovat o problémech spojených s prováděním a formulovat konkrétní doporučení, která je třeba zohlednit prostřednictvím lepšího provádění stávajících pravidel.

Pozměňovací návrh 21

Návrh směrnice
Bod odůvodnění 34

Znění navržené Komisí	*Pozměňovací návrh*
(34) Skupina pro spolupráci by i nadále měla být flexibilním fórem a měla by být schopna reagovat na měnící se a nové priority a výzvy politik, a přitom brát v úvahu dostupnost zdrojů. Měla by organizovat pravidelná společná setkání s relevantními soukromými zúčastněnými stranami z celé Unie za účelem projednání činností prováděných skupinou a shromažďování vstupů týkajících se vznikajících politických výzev. S cílem posílit spolupráci na úrovni Unie by skupina měla ***zvážit pozvání*** k účasti na ***její*** činnosti ***pro*** instituce a agentury Unie	(34) Skupina pro spolupráci by i nadále měla být flexibilním fórem a měla by být schopna reagovat na měnící se a nové priority a výzvy politik, a přitom brát v úvahu dostupnost zdrojů. Měla by organizovat pravidelná společná setkání s relevantními soukromými zúčastněnými stranami z celé Unie za účelem projednání činností prováděných skupinou a shromažďování vstupů týkajících se vznikajících politických výzev. S cílem posílit spolupráci na úrovni Unie by skupina měla ***pozvat*** k účasti na ***své*** činnosti ***relevantní*** instituce a agentury

zapojené do politiky v oblasti kybernetické bezpečnosti, ***jako je Evropské centrum pro boj proti kyberkriminalitě (EC3)***, ***Agentura*** Evropské unie pro bezpečnost letectví (EASA) a ***Agentura*** Evropské unie pro kosmický program (EUSPA).	Unie zapojené do politiky v oblasti kybernetické bezpečnosti, ***zejména Europol***, ***Agenturu*** Evropské unie pro bezpečnost letectví (EASA) a ***Agenturu*** Evropské unie pro kosmický program (EUSPA).

Pozměňovací návrh 22

Návrh směrnice
Bod odůvodnění 36

Znění navržené Komisí	*Pozměňovací návrh*
(36) Unie by ve vhodných případech měla v souladu s článkem 218 SFEU uzavírat mezinárodní dohody s třetími zeměmi nebo mezinárodními organizacemi, které umožní a zorganizují jejich účast na některých činnostech skupiny pro spolupráci a sítě CSIRT. ***Takové dohody*** by ***měly zajistit odpovídající ochranu údajů***.	(36) Unie by ve vhodných případech měla v souladu s článkem 218 SFEU uzavírat mezinárodní dohody s třetími zeměmi nebo mezinárodními organizacemi, které umožní a zorganizují jejich účast na některých činnostech skupiny pro spolupráci a sítě CSIRT. ***Pokud jsou osobní údaje předávány do třetí země nebo mezinárodní organizaci, měla*** by ***se použít kapitola V nařízení (EU) 2016/679***.

Pozměňovací návrh 23

Návrh směrnice
Bod odůvodnění 37

Znění navržené Komisí	*Pozměňovací návrh*
(37) Členské státy by měly přispět k vytvoření rámce EU pro reakci na kybernetické bezpečnostní krize uvedeného v doporučení (EU) 2017/1584 prostřednictvím stávajících sítí pro spolupráci, zejména sítě styčných organizací pro kybernetické krize (EU-CyCLONe), sítě CSIRT a skupiny pro spolupráci. Sítě EU-CyCLONe a CSIRT by měly spolupracovat na základě procesních ujednání, jež vymezí podmínky této spolupráce. Jednací řád sítě EU-CyCLONe by měl dále vymezit podmínky,	(37) Členské státy by měly přispět k vytvoření rámce EU pro reakci na kybernetické bezpečnostní krize uvedeného v doporučení (EU) 2017/1584 prostřednictvím stávajících sítí pro spolupráci, zejména sítě styčných organizací pro kybernetické krize (EU-CyCLONe), sítě CSIRT a skupiny pro spolupráci. Sítě EU-CyCLONe a CSIRT by měly spolupracovat na základě procesních ujednání, jež vymezí podmínky této spolupráce. Jednací řád sítě EU-CyCLONe by měl dále vymezit podmínky,

za nichž by měla síť fungovat, mimo jiné včetně úloh, způsobů spolupráce, interakcí s jinými relevantními subjekty a šablon pro sdílení informací, jakož i způsobů komunikace. Pokud jde o krizové řízení na úrovni Unie, měly by příslušné strany vycházet z integrovaných opatření pro politickou reakci na krize. Komise by za tímto účelem měla využít proces meziodvětvové koordinace na vysoké úrovni v krizových situacích ARGUS. Pokud má krize významný externí rozměr nebo rozměr společné bezpečnostní a obranné politiky (SBOP), měl by být aktivován mechanismus Evropské služby pro vnější činnost (ESVČ) pro reakce na krize.

za nichž by měla síť fungovat, mimo jiné včetně úloh, způsobů spolupráce, interakcí s jinými relevantními subjekty a šablon pro sdílení informací, jakož i způsobů komunikace. Pokud jde o krizové řízení na úrovni Unie, měly by příslušné strany vycházet z integrovaných opatření pro politickou reakci na krize. Komise by za tímto účelem měla využít proces meziodvětvové koordinace na vysoké úrovni v krizových situacích ARGUS. Pokud ***se krize týká dvou nebo více členských států a existuje podezření, že je trestní povahy, měla by být zvážena aktivace protokolu EU o vymáhání práva v případě nouze. Pokud*** má krize významný externí rozměr nebo rozměr společné bezpečnostní a obranné politiky (SBOP), měl by být aktivován mechanismus Evropské služby pro vnější činnost (ESVČ) pro reakce na krize.

Pozměňovací návrh 24

Návrh směrnice
Bod odůvodnění 45

Znění navržené Komisí	*Pozměňovací návrh*
(45) Subjekty by rovněž měly řešit kybernetická bezpečnostní rizika vyplývající z jejich interakcí a vztahů s jinými zúčastněnými stranami v rámci širšího ekosystému. Subjekty by zejména měly přijetím vhodných opatření zajistit, že jejich spolupráce s akademickými a výzkumnými institucemi probíhá v souladu s jejich politikami kybernetické bezpečnosti a řídí se osvědčenými postupy, pokud jde o bezpečný přístup a šíření informací obecně a ochranu duševního vlastnictví zvláště. Podobně by subjekty, jsou-li závislé na službách transformace dat a analýzy dat poskytovaných třetími stranami, vzhledem k důležitosti a hodnotě dat pro ***jejich*** činnost měly přijmout veškerá vhodná opatření v oblasti kybernetické bezpečnosti.	(45) Subjekty by rovněž měly řešit kybernetická bezpečnostní rizika vyplývající z jejich interakcí a vztahů s jinými zúčastněnými stranami v rámci širšího ekosystému. Subjekty by zejména měly přijetím vhodných opatření zajistit, že jejich spolupráce s akademickými a výzkumnými institucemi probíhá v souladu s jejich politikami kybernetické bezpečnosti a řídí se osvědčenými postupy, pokud jde o bezpečný přístup a šíření informací obecně a ochranu duševního vlastnictví zvláště. Podobně by subjekty, jsou-li závislé na službách transformace dat a analýzy dat poskytovaných třetími stranami, vzhledem k důležitosti a hodnotě dat pro ***svou*** činnost měly přijmout veškerá vhodná opatření v oblasti kybernetické bezpečnosti ***a hlásit všechny potenciální***

kybernetické útoky, které odhalí.

Pozměňovací návrh 25

Návrh směrnice
Bod odůvodnění 46 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(46a) Zvláštní pozornost by měla být věnována skutečnosti, že služby, systémy nebo produkty IKT, které podléhají zvláštním požadavkům v zemi původu, by mohly představovat překážku pro dodržování právních předpisů EU v oblasti ochrany soukromí a ochrany údajů. V případě potřeby by měl být v rámci takovýchto posouzení rizik konzultován Evropský sbor pro ochranu osobních údajů. Svobodný software a software s otevřeným zdrojovým kódem, jakož i hardware s otevřeným zdrojovým kódem by mohly přinést obrovské výhody z hlediska kybernetické bezpečnosti, zejména pokud jde o transparentnost a ověřitelnost prvků. Jelikož by to mohlo pomoci řešit a zmírnit konkrétní rizika v dodavatelském řetězci, mělo by být jejich využívání upřednostněno tam, kde je to proveditelné v souladu se stanoviskem evropského inspektora ochrany údajů č. 5/2021[1a].
	[1a] Stanovisko Evropského inspektora ochrany údajů č. 5/2021 ke strategii kybernetické bezpečnosti EU a směrnici NIS 2, 11. března 2021.

Pozměňovací návrh 26

Návrh směrnice
Bod odůvodnění 47

Znění navržené Komisí	*Pozměňovací návrh*
(47) Posouzení rizik dodavatelského	(47) Posouzení rizik dodavatelského

řetězce by s ohledem na charakteristické rysy dotčeného odvětví měla zohlednit jak technické, tak případné netechnické faktory ***včetně faktorů vymezených*** v doporučení (EU) 2019/534, v koordinovaném posouzení rizik pro bezpečnost sítí 5G v celé EU a v souboru opatření EU pro kybernetickou bezpečnost sítí 5G, na němž se dohodla skupina pro spolupráci. K určení dodavatelských řetězců, které by měly podléhat koordinovanému posouzení rizik, by měla být vzata v úvahu tato kritéria: i) rozsah, v jakém základní a důležité subjekty využívají konkrétní kritické služby, systémy a produkty IKT a jsou na nich závislé; ii) relevantnost konkrétních služeb, systémů nebo produktů IKT pro plnění kritických nebo citlivých funkcí, včetně zpracování osobních údajů; iii) dostupnost alternativních služeb, systémů nebo produktů IKT; iv) odolnost celého dodavatelského řetězce služeb, systémů nebo produktů IKT vůči narušení a v) u vznikajících služeb, systémů nebo produktů IKT jejich budoucí význam pro činnost subjektů.	řetězce by s ohledem na charakteristické rysy dotčeného odvětví měla zohlednit jak technické, tak případné netechnické faktory***, které by měly být dále upřesněny koordinační skupinou a k nimž patří faktory vymezené*** v doporučení (EU) 2019/534, v koordinovaném posouzení rizik pro bezpečnost sítí 5G v celé EU a v souboru opatření EU pro kybernetickou bezpečnost sítí 5G, na němž se dohodla skupina pro spolupráci. K určení dodavatelských řetězců, které by měly podléhat koordinovanému posouzení rizik, by měla být vzata v úvahu tato kritéria: i) rozsah, v jakém základní a důležité subjekty využívají konkrétní kritické služby, systémy a produkty IKT a jsou na nich závislé; ii) relevantnost konkrétních služeb, systémů nebo produktů IKT pro plnění kritických nebo citlivých funkcí, včetně zpracování osobních údajů; iii) dostupnost alternativních služeb, systémů nebo produktů IKT; iv) odolnost celého dodavatelského řetězce služeb, systémů nebo produktů IKT vůči narušení a v) u vznikajících služeb, systémů nebo produktů IKT jejich budoucí význam pro činnost subjektů.

Pozměňovací návrh 27

Návrh směrnice
Bod odůvodnění 48 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(48a) Malé a střední podniky často nemají velikost a zdroje nutné k tomu, aby mohly naplňovat širokou a zvětšující se škálu potřeb v oblasti kybernetické bezpečnosti v propojeném světě, kdy navíc dochází k nárůstu práce na dálku. Členské státy by se proto měly ve svých vnitrostátních strategiích v oblasti kybernetické bezpečnosti zabývat pokyny pro malé a střední podniky a jejich podporou.

Pozměňovací návrh 28

Návrh směrnice
Bod odůvodnění 50

Znění navržené Komisí	*Pozměňovací návrh*
(50) Vzhledem k rostoucímu významu interpersonálních komunikačních služeb nezávislých na číslech je nutné zajistit, aby i tyto služby podléhaly odpovídajícím bezpečnostním požadavkům v souladu s jejich zvláštní povahou a ekonomickým významem. Provozovatelé takových služeb by tedy měli rovněž zajišťovat úroveň ***bezpečnosti sítí a informačních systémů*** odpovídající existující míře rizika. Vzhledem k tomu, že poskytovatelé interpersonálních komunikačních služeb nezávislých na číslech obvykle nevykonávají skutečnou kontrolu nad přenosem signálů v sítích, lze míru rizika pro tyto služby v některých ohledech považovat za nižší než v případě tradičních služeb elektronických komunikací. Totéž platí o interpersonálních komunikačních službách, které využívají čísla a které nevykonávají skutečnou kontrolu nad přenosem signálů.	(50) Vzhledem k rostoucímu významu interpersonálních komunikačních služeb nezávislých na číslech je nutné zajistit, aby i tyto služby podléhaly odpovídajícím bezpečnostním požadavkům v souladu s jejich zvláštní povahou a ekonomickým významem. Provozovatelé takových služeb by tedy měli rovněž zajišťovat úroveň ***kybernetické bezpečnosti*** odpovídající existující míře rizika. Vzhledem k tomu, že poskytovatelé interpersonálních komunikačních služeb nezávislých na číslech obvykle nevykonávají skutečnou kontrolu nad přenosem signálů v sítích, lze míru rizika pro tyto služby v některých ohledech považovat za nižší než v případě tradičních služeb elektronických komunikací. Totéž platí o interpersonálních komunikačních službách, které využívají čísla a které nevykonávají skutečnou kontrolu nad přenosem signálů.

Pozměňovací návrh 29

Návrh směrnice
Bod odůvodnění 52

Znění navržené Komisí	*Pozměňovací návrh*
(52) Ve vhodných případech by subjekty měly informovat příjemce svých služeb o konkrétních a závažných hrozbách a o opatřeních, která mohou přijmout, aby snížili riziko, jež jim z těchto hrozeb vyplývá. Požadavek na informování příjemců o hrozbách by subjekty neměl zbavovat povinnosti přijmout na své vlastní náklady přiměřená a okamžitá opatření s cílem zamezit jakýmkoli kybernetickým hrozbám nebo je odstranit a obnovit běžnou úroveň bezpečnosti služby. Tyto	(52) Ve vhodných případech by subjekty měly ***mít možnost*** informovat příjemce svých služeb o konkrétních a závažných hrozbách a o opatřeních, která mohou přijmout, aby snížili riziko, jež jim z těchto hrozeb vyplývá. Požadavek na informování příjemců o hrozbách by subjekty neměl zbavovat povinnosti přijmout na své vlastní náklady přiměřená a okamžitá opatření s cílem zamezit jakýmkoli kybernetickým hrozbám nebo je odstranit a obnovit běžnou úroveň bezpečnosti služby. Tyto

informace o bezpečnostních hrozbách by měly být příjemcům poskytovány zdarma.	informace o bezpečnostních hrozbách by měly být příjemcům poskytovány zdarma.

Pozměňovací návrh 30

Návrh směrnice
Bod odůvodnění 53

Znění navržené Komisí	*Pozměňovací návrh*
(53) Poskytovatelé veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací by měli příjemce služby ***zejména*** informovat o konkrétních a závažných kybernetických hrozbách a o opatřeních, která mohou přijmout, aby chránili bezpečnost ***své*** komunikace, například použitím specifických druhů softwaru nebo šifrovacích technologií.	(53) Poskytovatelé veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací by měli ***zejména uplatňovat bezpečnost již od fáze návrhu a standardní bezpečnost a měli by mít možnost*** příjemce služby informovat o konkrétních a závažných kybernetických hrozbách a o opatřeních, která mohou přijmout, aby chránili bezpečnost ***svých zařízení a*** komunikace, například použitím specifických druhů softwaru nebo šifrovacích technologií. ***V zájmu zvýšení bezpečnosti hardwaru a softwaru by poskytovatelé měli být vybízeni k tomu, aby používali hardware s otevřeným designem nebo otevřený hardware.***

Pozměňovací návrh 31

Návrh směrnice
Bod odůvodnění 54

Znění navržené Komisí	*Pozměňovací návrh*
(54) S cílem zajistit bezpečnost sítí a služeb elektronické komunikace by mělo být podporováno použití šifrování, a zejména šifrování mezi koncovými body, a v případě nutnosti by pro poskytovatele těchto služeb a sítí v souladu se zásadami bezpečnosti a soukromí standardně a záměrně pro účely článku 18 mělo být povinné. Použití šifrování mezi koncovými body by mělo být v souladu s ***pravomocemi*** členských států zajistit ochranu podstatných zájmů své	(54) S cílem zajistit bezpečnost sítí a služeb elektronické komunikace***, jakož i základní práva na ochranu údajů a soukromí*** by mělo být podporováno použití šifrování, a zejména šifrování mezi koncovými body, a v případě nutnosti by pro poskytovatele těchto služeb a sítí v souladu se zásadami bezpečnosti a soukromí standardně a záměrně pro účely článku 18 mělo být povinné. Použití šifrování mezi koncovými body by mělo být v souladu s ***odpovědností*** členských

bezpečnosti a veřejné bezpečnosti a umožnit vyšetřování, odhalování a stíhání trestných činů v souladu s právem Unie. Řešení k zajištění zákonného přístupu k informacím v rámci komunikace šifrované mezi koncovými body by měla zachovat účinnost šifrování při ochraně soukromí a bezpečnosti komunikací, a ***současně poskytnout účinnou reakci*** na ***trestnou činnost***.

států zajistit ochranu podstatných zájmů své bezpečnosti a veřejné bezpečnosti a umožnit ***prevenci,*** vyšetřování, odhalování a stíhání trestných činů v souladu s právem Unie ***a s vnitrostátním právem***. Řešení k zajištění zákonného přístupu k informacím v rámci komunikace šifrované mezi koncovými body by měla zachovat účinnost šifrování při ochraně soukromí a bezpečnosti komunikací***.*** ***Žádné ustanovení tohoto nařízení by nemělo být vnímáno jako úsilí o oslabení šifrování mezi koncovými body prostřednictvím „zadních vrátek“ („backdoors“) nebo podobných řešení, neboť nedostatky v šifrování mohou být zneužívány k nekalým účelům. Jakákoli opatření zaměřená na oslabení šifrování nebo obcházení architektury technologie mohou představovat značná rizika pro účinné ochranné kapacity této technologie. Mělo by být zakázáno jakékoli nepovolené dešifrování nebo sledování elektronických komunikací s výjimkou sledování právními orgány, aby se zajistila účinnost technologie*** a ***její širší využití. Je důležité, aby členské státy řešily problémy, s nimiž se setkávají právní orgány i subjekty provádějící výzkum zranitelných míst. V některých členských státech jsou subjekty i fyzické osoby provádějící výzkum zranitelných míst vystaveny trestněprávní a občanskoprávní odpovědnosti. Členské státy se proto vyzývají, aby vydaly pokyny, na jejichž základě by byl výzkum informační bezpečnosti vyňat z trestního stíhání a odpovědnosti.***

Pozměňovací návrh 32

Návrh směrnice
Bod odůvodnění 56

Znění navržené Komisí	*Pozměňovací návrh*
(56) Základní a důležité subjekty jsou často v situaci, kdy je konkrétní incident	(56) Základní a důležité subjekty jsou často v situaci, kdy je konkrétní incident

vzhledem k jeho povaze třeba v důsledku oznamovacích povinností uvedených v různých právních nástrojích ohlásit různým orgánům. Takové případy vytvářejí další zátěž a mohou také vést k nejasnostem, pokud jde o formát a postupy takových oznámení. Vzhledem k tomu a za účelem zjednodušení hlášení o bezpečnostních incidentech by členské státy měly stanovit jedno vstupní místo ***pro všechna oznámení vyžadovaná*** podle této směrnice i podle jiných právních předpisů Unie, jako je nařízení (EU) 2016/679 a směrnice 2002/58/ES. Agentura ENISA by ve spolupráci se skupinou pro spolupráci měla vypracovat společné šablony hlášení prostřednictvím pokynů, které by zjednodušily a zefektivnily informace uvedené v hlášeních, jež vyžaduje právo Unie, a snížily zátěž pro společnosti.	vzhledem k jeho povaze třeba v důsledku oznamovacích povinností uvedených v různých právních nástrojích ohlásit různým orgánům. Takové případy vytvářejí další zátěž a mohou také vést k nejasnostem, pokud jde o formát a postupy takových oznámení. Vzhledem k tomu a za účelem zjednodušení hlášení o bezpečnostních incidentech by členské státy měly stanovit jedno vstupní místo ***vyžadované*** podle této směrnice i podle jiných právních předpisů Unie, jako je nařízení (EU) 2016/679 a směrnice 2002/58/ES. Agentura ENISA by ve spolupráci se skupinou pro spolupráci ***a Evropským sborem pro ochranu osobních údajů*** měla vypracovat společné šablony hlášení prostřednictvím pokynů, které by zjednodušily a zefektivnily informace uvedené v hlášeních, jež vyžaduje právo Unie, a snížily zátěž pro společnosti.

Pozměňovací návrh 33

Návrh směrnice
Bod odůvodnění 57

Znění navržené Komisí	*Pozměňovací návrh*
(57) Existuje-li podezření, že určitý incident souvisí se závažnou trestnou činností podle unijního nebo vnitrostátního práva, měly by členské státy motivovat základní a důležité subjekty, aby na základě platných pravidel trestního řízení v souladu s právem Unie incidenty s podezřením na trestní povahu ohlašovaly z vlastní iniciativy donucovacím orgánům. V případě potřeby, a aniž jsou dotčena pravidla ochrany osobních údajů platná pro Europol, je žádoucí, aby koordinaci mezi příslušnými orgány a donucovacími orgány v různých členských státech usnadnily EC3 a agentura ENISA.	(57) Existuje-li podezření, že určitý incident souvisí se závažnou trestnou činností podle unijního nebo vnitrostátního práva, měly by členské státy motivovat základní a důležité subjekty, aby na základě platných pravidel trestního řízení v souladu s právem Unie incidenty s podezřením na trestní povahu ohlašovaly z vlastní iniciativy donucovacím orgánům. V případě potřeby, a aniž jsou dotčena pravidla ochrany osobních údajů platná pro Europol, je žádoucí, aby koordinaci mezi příslušnými orgány a donucovacími orgány v různých členských státech usnadnily ***Evropské centrum pro boj proti kyberkriminalitě (***EC3***) Europolu*** a agentura ENISA.

Pozměňovací návrh 34

Návrh směrnice
Bod odůvodnění 58

Znění navržené Komisí	*Pozměňovací návrh*
(58) V důsledku incidentů je v mnoha případech ohrožena ochrana osobních údajů. V této souvislosti by příslušné orgány měly spolupracovat s orgány pro ochranu osobních údajů a orgány dozoru podle směrnice 2002/58/ES a vyměňovat si s nimi informace o všech relevantních záležitostech	(58) V důsledku incidentů je v mnoha případech ohrožena ochrana osobních údajů. V této souvislosti by příslušné orgány měly spolupracovat s orgány pro ochranu osobních údajů a ***dozorovými úřady a*** orgány dozoru podle ***nařízení (EU) 2016/679 a*** směrnice 2002/58/ES a vyměňovat si s nimi informace o všech relevantních záležitostech***.***

Pozměňovací návrh 35

Návrh směrnice
Bod odůvodnění 59

Znění navržené Komisí	*Pozměňovací návrh*
(59) Udržování přesných a úplných databází doménových jmen a registračních údajů (takzvaných „údajů WHOIS“) a poskytování zákonného přístupu k těmto údajům má zásadní význam pro zajištění bezpečnosti, stability a odolnosti systému doménových jmen (DNS), což na druhé straně přispívá k vyšší společné úrovni kybernetické bezpečnosti v Unii. Pokud zpracování údajů zahrnuje osobní údaje, musí takové zpracování být v souladu s ***právem*** Unie v oblasti ochrany údajů.	(59) Udržování přesných a úplných databází doménových jmen a registračních údajů (takzvaných „údajů WHOIS“) a poskytování zákonného přístupu k těmto údajům má zásadní význam pro zajištění bezpečnosti, stability a odolnosti systému doménových jmen (DNS), což na druhé straně přispívá k vyšší společné úrovni kybernetické bezpečnosti v Unii. Pokud zpracování údajů zahrnuje osobní údaje, musí takové zpracování být v souladu s ***platnými právními předpisy*** Unie v oblasti ochrany údajů.

Pozměňovací návrh 36

Návrh směrnice
Bod odůvodnění 62

Znění navržené Komisí	*Pozměňovací návrh*
(62) ***Registry*** internetových domén nejvyšší úrovně a subjekty poskytující jim	(62) ***Za účelem splnění své právní povinnosti podle čl. 6 odst. 1 písm. c) a čl.***

služby registrace domén ***by*** měly veřejně zpřístupnit údaje o registraci domén***, které nespadají do oblasti působnosti pravidel Unie*** na ***ochranu osobních údajů***, například ***údajů, které se týkají právnických osob***[25]. Registry internetových domén nejvyšší úrovně a subjekty poskytující služby registrace domén nejvyšší úrovně by také měly ***v souladu s právem Unie na ochranu osobních údajů umožnit oprávněným žadatelům o přístup*** zákonný přístup ke konkrétním údajům o registraci domén týkajícím se fyzických osob. Členské státy by měly zajistit, aby registry internetových domén nejvyšší úrovně a subjekty poskytující jim služby registrace domén bez zbytečného odkladu reagovaly na žádosti ***oprávněných žadatelů o přístup*** o zpřístupnění údajů o registraci domén. Registry internetových domén nejvyšší úrovně a subjekty poskytující jim služby registrace domén by měly stanovit politiky a postupy pro zveřejňování a zpřístupnění registračních údajů, včetně dohod o úrovni služeb k vyřizování žádostí o přístup od oprávněných žadatelů o přístup. Postup poskytování přístupu může také obsahovat užívání rozhraní, portálu nebo jiného technického nástroje k zajištění účinného systému žádostí o registrační údaje a přístupu k těmto údajům. Za účelem podpory harmonizovaných postupů na vnitřním trhu může Komise přijmout pokyny o takových postupech, aniž jsou dotčeny pravomoci Evropského sboru pro ochranu osobních údajů.

6 odst. 3 nařízení (EU) 2016/679 by registry internetových domén nejvyšší úrovně a subjekty poskytující jim služby registrace domén měly veřejně zpřístupnit ***některé*** údaje o registraci domén ***stanovené v právních předpisech členského státu, které se*** na ***ně vztahují***, například ***doménové jméno a název právnické osoby***. Registry internetových domén nejvyšší úrovně a subjekty poskytující služby registrace domén nejvyšší úrovně by také měly ***umožnit oprávněným žadatelům o přístup, zejména příslušným orgánům podle této směrnice nebo dozorovým úřadům podle nařízení (EU) 2016/679 v souladu s jejich pravomocemi,*** zákonný přístup ke konkrétním údajům o registraci domén týkajícím se fyzických osob. Členské státy by měly zajistit, aby registry internetových domén nejvyšší úrovně a subjekty poskytující jim služby registrace domén bez zbytečného odkladu reagovaly na ***zákonné a řádně odůvodněné*** žádosti ***veřejných orgánů, včetně příslušných orgánů podle této směrnice, příslušných orgánů podle unijního nebo vnitrostátního práva pro prevenci, vyšetřování či stíhání trestných činů nebo dozorových úřadů podle nařízení (EU) 2016/679,*** o zpřístupnění údajů o registraci domén. Registry internetových domén nejvyšší úrovně a subjekty poskytující jim služby registrace domén by měly stanovit politiky a postupy pro zveřejňování a zpřístupnění registračních údajů, včetně dohod o úrovni služeb k vyřizování žádostí o přístup od oprávněných žadatelů o přístup. Postup poskytování přístupu může také obsahovat užívání rozhraní, portálu nebo jiného technického nástroje k zajištění účinného systému žádostí o registrační údaje a přístupu k těmto údajům. Za účelem podpory harmonizovaných postupů na vnitřním trhu může Komise přijmout pokyny o takových postupech, aniž jsou dotčeny pravomoci Evropského sboru pro ochranu osobních

údajů.

_____ _____

[25] Viz 14. bod odůvodnění NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679, kde se uvádí, že „toto nařízení se nevztahuje na zpracování osobních údajů právnických osob, a zejména podniků vytvořených jako právnické osoby, včetně názvu, právní formy a kontaktních údajů právnické osoby“.

Pozměňovací návrh 37

Návrh směrnice
Bod odůvodnění 63

Znění navržené Komisí	*Pozměňovací návrh*
(63) ***Všechny*** základní a důležité subjekty podle této směrnice ***by*** měly podléhat pravomoci členského státu, ve kterém poskytují své služby. Poskytuje-li subjekt služby ve více než jednom členském státě, měl by podléhat samostatné a souběžné pravomoci každého z těchto členských států. Příslušné orgány těchto členských států by měly spolupracovat, poskytovat si navzájem pomoc a v případě potřeby provádět společné akce v oblasti dohledu.	(63) ***Pro účely této směrnice by všechny*** základní a důležité subjekty podle této směrnice měly podléhat pravomoci členského státu, ve kterém poskytují své služby. Poskytuje-li subjekt služby ve více než jednom členském státě, měl by podléhat samostatné a souběžné pravomoci každého z těchto členských států. Příslušné orgány těchto členských států by ***se*** měly ***dohodnout na základních klasifikacích,*** spolupracovat, ***kdykoli to bude možné,*** poskytovat si navzájem ***v reálném čase*** pomoc a v případě potřeby provádět společné akce v oblasti dohledu.

Pozměňovací návrh 38

Návrh směrnice
Bod odůvodnění 64

Znění navržené Komisí	*Pozměňovací návrh*
(64) S cílem zohlednit přeshraniční povahu služeb a činností poskytovatelů služeb systému doménových jmen, registrů internetových domén nejvyšší úrovně, poskytovatelů sítí pro doručování obsahu,	(64) S cílem zohlednit přeshraniční povahu služeb a činností poskytovatelů služeb systému doménových jmen, registrů internetových domén nejvyšší úrovně, poskytovatelů sítí pro doručování obsahu,

poskytovatelů služeb cloud computingu, poskytovatelů služeb datových center a poskytovatelů digitálních služeb by pravomoc nad těmito subjekty měl mít pouze jeden členský stát. ***Pravomoc*** by měl mít ten členský stát, v němž má daný subjekt v rámci Unie hlavní místo obchodní činnosti. Kritérium místa obchodní činnosti pro účely této směrnice předpokládá účinný výkon činnosti prostřednictvím stálých struktur. Právní forma takových struktur, ať již jde o pobočku, nebo dceřinou společnost s právní subjektivitou, není v tomto ohledu rozhodujícím faktorem. To, zda je toto kritérium splněno, by nemělo záviset na tom, zda se sítě a informační systémy fyzicky nacházejí na daném místě; sama přítomnost a samotné používání takových sítí a systémů nejsou podstatou hlavního místa obchodní činnosti, a tudíž ani nejsou rozhodujícími kritérii pro jeho určení. Hlavní místo obchodní činnosti by mělo být místo v Unii, kde jsou přijímána rozhodnutí týkající se opatření k řízení kybernetických bezpečnostních rizik. To bude obvykle odpovídat místu, kde se nachází ústřední správa společnosti v Unii. Pokud taková rozhodnutí nejsou v Unii přijímána, mělo by se mít za to, že hlavní místo obchodní činnosti je v členském státě, ve kterém má subjekt provozovnu s nejvyšším počtem zaměstnanců v Unii. Pokud jsou služby prováděny skupinou podniků, mělo by se za hlavní místo obchodní činnosti skupiny podniků považovat hlavní místo obchodní činnosti řídícího podniku.

poskytovatelů služeb cloud computingu, poskytovatelů služeb datových center a poskytovatelů digitálních služeb by pravomoc nad těmito subjekty měl mít pouze jeden členský stát. ***Pro účely této směrnice*** by ***pravomoc*** měl mít ten členský stát, v němž má daný subjekt v rámci Unie hlavní místo obchodní činnosti. Kritérium místa obchodní činnosti pro účely této směrnice předpokládá účinný výkon činnosti prostřednictvím stálých struktur. Právní forma takových struktur, ať již jde o pobočku, nebo dceřinou společnost s právní subjektivitou, není v tomto ohledu rozhodujícím faktorem. To, zda je toto kritérium splněno, by nemělo záviset na tom, zda se sítě a informační systémy fyzicky nacházejí na daném místě; sama přítomnost a samotné používání takových sítí a systémů nejsou podstatou hlavního místa obchodní činnosti, a tudíž ani nejsou rozhodujícími kritérii pro jeho určení. Hlavní místo obchodní činnosti by mělo být místo v Unii, kde jsou přijímána rozhodnutí týkající se opatření k řízení kybernetických bezpečnostních rizik. To bude obvykle odpovídat místu, kde se nachází ústřední správa společnosti v Unii. Pokud taková rozhodnutí nejsou v Unii přijímána, mělo by se mít za to, že hlavní místo obchodní činnosti je v členském státě, ve kterém má subjekt provozovnu s nejvyšším počtem zaměstnanců v Unii. Pokud jsou služby prováděny skupinou podniků, mělo by se za hlavní místo obchodní činnosti skupiny podniků považovat hlavní místo obchodní činnosti řídícího podniku.

Pozměňovací návrh 39

Návrh směrnice
Bod odůvodnění 69

Znění navržené Komisí	*Pozměňovací návrh*
(69) Zpracování osobních údajů v rozsahu nezbytně nutném a přiměřeném	(69) Zpracování osobních údajů v rozsahu nezbytně nutném a přiměřeném

pro zajištění bezpečnosti sítí a informací ***ze strany subjektů***, které provádějí orgány veřejné správy, týmy CERT, týmy CSIRT a poskytovatelé bezpečnostních technologií a služeb, by mělo představovat oprávněný zájem dotčeného správce údajů podle nařízení (EU) 2016/679. To by mělo zahrnovat opatření týkající se prevence, odhalování a analýzy incidentů a reakce na incidenty, opatření ke zvyšování povědomí o konkrétních kybernetických hrozbách, výměnu informací v rámci odstraňování a koordinovaného odhalování zranitelných míst, a také dobrovolnou výměnu informací o těchto incidentech, kybernetických hrozbách a zranitelných místech, indikátorech narušení, taktice, technikách a postupech, varováních v oblasti kybernetické bezpečnosti a konfiguračních nástrojích. Taková opatření mohou vyžadovat zpracovávání ***těchto druhů*** osobních údajů***:*** IP adres, jednotných adres zdroje (URL), doménových jmen a e-mailových adres.

pro zajištění bezpečnosti sítí a informací, které provádějí ***subjekty,*** orgány veřejné správy, týmy CERT, týmy CSIRT a poskytovatelé bezpečnostních technologií a služeb, ***je nezbytné k tomu, aby mohli plnit své právní povinnosti podle vnitrostátních právních předpisů, jež provádějí tuto směrnici, a vztahují se na něj proto čl. 6 odst. 1 písm. c) a čl. 6 odst. 3 nařízení (EU) 2016/679.***

Toto zpracování by ***navíc*** mělo představovat oprávněný zájem dotčeného správce údajů podle ***čl. 6 odst. 1 písm. f)*** nařízení (EU) 2016/679. To by mělo zahrnovat opatření týkající se prevence, odhalování a analýzy incidentů a reakce na incidenty, opatření ke zvyšování povědomí o konkrétních kybernetických hrozbách, výměnu informací v rámci odstraňování a koordinovaného odhalování zranitelných míst, a také dobrovolnou výměnu informací o těchto incidentech, kybernetických hrozbách a zranitelných místech, indikátorech narušení, taktice, technikách a postupech, varováních v oblasti kybernetické bezpečnosti a konfiguračních nástrojích. ***V mnoha případech jsou osobní údaje ohroženy v důsledku kybernetických incidentů, a proto by příslušné orgány a orgány pro ochranu údajů členských států EU měly spolupracovat a vyměňovat si informace o všech relevantních záležitostech s cílem jakékoli porušení ochrany osobních údajů řešit.*** Taková opatření mohou vyžadovat zpracovávání ***některých kategorií*** osobních údajů***, včetně*** IP adres, jednotných adres zdroje (URL), doménových jmen a e-mailových adres.

Pozměňovací návrh 40

Návrh směrnice
Bod odůvodnění 71

Znění navržené Komisí	*Pozměňovací návrh*
(71) K zajištění účinného vymáhání by	(71) K zajištění účinného vymáhání by

měl být stanoven minimální seznam správních sankcí za porušení povinnosti v oblasti řízení kybernetických bezpečnostních rizik a hlášení, jež stanoví tato směrnice, čímž se vytvoří jasný a jednotný rámec pro takové sankce v celé Unii. Náležitá pozornost by měla být věnována ***povaze,*** závažnosti a době trvání protiprávního jednání, skutečné způsobené škodě či ztrátám nebo potenciálním škodám či ztrátám, které mohly být vyvolány, úmyslné nebo nedbalostní povaze protiprávního jednání, opatřením přijatým za účelem prevence nebo zmenšení způsobené škody nebo ztrát, míře odpovědnosti nebo jakémukoli relevantnímu protiprávnímu jednání v minulosti, míře spolupráce s příslušným orgánem a jakýmkoli jiným přitěžujícím nebo polehčujícím faktorům. ***Uložení sankcí*** včetně správních pokut by ***mělo*** podléhat vhodným procesním zárukám v souladu s obecnými zásadami práva Unie a Listinou základních práv Evropské unie, včetně účinné právní ochrany a spravedlivého procesu.

měl být stanoven minimální seznam správních sankcí za porušení povinnosti v oblasti řízení kybernetických bezpečnostních rizik a hlášení, jež stanoví tato směrnice, čímž se vytvoří jasný a jednotný rámec pro takové sankce v celé Unii. Náležitá pozornost by měla být věnována závažnosti a době trvání protiprávního jednání, skutečné způsobené škodě či ztrátám nebo potenciálním škodám či ztrátám, které mohly být vyvolány, ***jakémukoli relevantnímu předchozímu protiprávnímu jednání, způsobu, jakým se příslušný orgán o daném protiprávním jednání dozvěděl,*** úmyslné nebo nedbalostní povaze protiprávního jednání, opatřením přijatým za účelem prevence nebo zmenšení způsobené škody nebo ztrát, míře odpovědnosti nebo jakémukoli relevantnímu protiprávnímu jednání v minulosti, míře spolupráce s příslušným orgánem a jakýmkoli jiným přitěžujícím nebo polehčujícím faktorům. ***Uložené sankce*** včetně správních pokut by ***měly*** podléhat vhodným procesním zárukám v souladu s obecnými zásadami práva Unie a Listinou základních práv Evropské unie, včetně účinné právní ochrany a spravedlivého procesu.

Pozměňovací návrh 41

Návrh směrnice
Bod odůvodnění 74

Znění navržené Komisí	*Pozměňovací návrh*
(74) Členským státům by mělo být umožněno, aby stanovily pravidla týkající se trestních sankcí za porušení vnitrostátních pravidel provádějících tuto směrnici. Uložení trestních sankcí za porušení těchto vnitrostátních pravidel a souvisejících správních sankcí by však nemělo vést k porušení zásady ne bis in idem, jak ji vykládá Soudní dvůr.	(74) Členským státům by mělo být umožněno, aby stanovily pravidla týkající se trestních sankcí za porušení vnitrostátních pravidel provádějících tuto směrnici. ***Tyto trestní sankce mohou rovněž zahrnovat odebrání zisků získaných na základě porušení tohoto nařízení.*** Uložení trestních sankcí za porušení těchto vnitrostátních pravidel a souvisejících správních sankcí by však

nemělo vést k porušení zásady ne bis in idem, jak ji vykládá Soudní dvůr.

Pozměňovací návrh 42

Návrh směrnice
Bod odůvodnění 76

Znění navržené Komisí	*Pozměňovací návrh*
(76) Aby se dále posílila účinnost a odrazující účinek sankcí, jež mají být uloženy za porušení povinností stanovených podle této směrnice, měly by být příslušné orgány oprávněny uplatňovat sankce spočívající v pozastavení osvědčení nebo povolení týkajícího se části nebo všech služeb, jež poskytuje základní subjekt***, a uložení dočasného zákazu výkonu řídící funkce fyzické osoby***. Vzhledem k závažnosti a dopadu těchto sankcí na činnost subjektů a v konečném důsledku na jejich zákazníky, měly by být uplatňovány pouze úměrně závažnosti porušení a s ohledem na konkrétní okolnosti každého případu, včetně úmyslné nebo nedbalostní povahy porušení, opatřením přijatým k zamezení nebo zmírnění způsobené škody nebo ztrát. Tyto sankce by se měly používat jen jako krajní prostředek, což znamená pouze po vyčerpání ostatních relevantních donucovacích opatření, jež stanoví tato směrnice, a pouze po dobu, než subjekty, vůči kterým jsou uplatněny, přijmou nezbytná opatření k nápravě nedostatků nebo k dosažení souladu s požadavky příslušného orgánu, kvůli kterým byly tyto sankce uloženy. Uložení takových sankcí musí podléhat vhodným procesním zárukám v souladu s obecnými zásadami práva Unie a Listiny základních práv Evropské unie, včetně ***účinné právní ochrany***, spravedlivého procesu, presumpce neviny a práva na obhajobu.	(76) Aby se dále posílila účinnost a odrazující účinek sankcí, jež mají být uloženy za porušení povinností stanovených podle této směrnice, měly by být příslušné orgány oprávněny uplatňovat sankce spočívající v pozastavení osvědčení nebo povolení týkajícího se části nebo všech služeb, jež poskytuje základní subjekt. Vzhledem k závažnosti a dopadu těchto sankcí na činnost subjektů a v konečném důsledku na jejich zákazníky, měly by být uplatňovány pouze úměrně závažnosti porušení a s ohledem na konkrétní okolnosti každého případu, včetně úmyslné nebo nedbalostní povahy porušení, opatřením přijatým k zamezení nebo zmírnění způsobené škody nebo ztrát. Tyto sankce by se měly používat jen jako krajní prostředek, což znamená pouze po vyčerpání ostatních relevantních donucovacích opatření, jež stanoví tato směrnice, a pouze po dobu, než subjekty, vůči kterým jsou uplatněny, přijmou nezbytná opatření k nápravě nedostatků nebo k dosažení souladu s požadavky příslušného orgánu, kvůli kterým byly tyto sankce uloženy. Uložení takových sankcí musí podléhat vhodným procesním zárukám v souladu s obecnými zásadami práva Unie a Listiny základních práv Evropské unie, včetně ***účinných opravných prostředků***, spravedlivého procesu, presumpce neviny a práva na obhajobu.

Pozměňovací návrh 43

Návrh směrnice
Bod odůvodnění 77

Znění navržené Komisí	*Pozměňovací návrh*
(77) Tato směrnice by měla stanovit pravidla spolupráce mezi příslušnými orgány a ***orgány dohledu v souladu s nařízením*** (EU) 2016/679 pro řešení případů porušení souvisejících s osobními údaji.	(77) Tato směrnice by měla stanovit pravidla spolupráce mezi příslušnými orgány ***podle této směrnice*** a ***dozorovými úřady podle nařízení*** (EU) 2016/679 pro řešení případů porušení souvisejících s osobními údaji.

Pozměňovací návrh 44

Návrh směrnice
Bod odůvodnění 79

Znění navržené Komisí	*Pozměňovací návrh*
(79) Měl by být zaveden mechanismus vzájemného hodnocení, který umožní, aby provádění politik kybernetické bezpečnosti, včetně úrovně schopností a dostupných zdrojů členských států, posuzovali odborníci určení členskými státy.	(79) Měl by být zaveden mechanismus vzájemného hodnocení, který umožní, aby provádění politik kybernetické bezpečnosti, včetně úrovně schopností a dostupných zdrojů členských států, posuzovali odborníci určení členskými státy. ***EU by měla usnadnit koordinovanou reakci na rozsáhlé kybernetické incidenty a krize a nabízet pomoc, aby přispěla k obnově po těchto kybernetických útocích.***

Pozměňovací návrh 45

Návrh směrnice
Bod odůvodnění 82 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(82a) Tato směrnice se nevztahuje na orgány, instituce a jiné subjekty Unie. Instituce Unie by však mohly být považovány za základní nebo důležité subjekty podle této směrnice. Aby se dosáhlo jednotné úrovně ochrany pomocí soudržných a homogenních pravidel, měla

by Komise do 31. prosince 2022 zveřejnit legislativní návrh na zahrnutí orgánů, institucí a jiných subjektů Unie do celounijního rámce pro kybernetickou bezpečnost.

Pozměňovací návrh 46

Návrh směrnice
Bod odůvodnění 84

Znění navržené Komisí	*Pozměňovací návrh*
(84) Tato směrnice dodržuje základní práva a ctí zásady uznané Listinou základních práv Evropské unie, zejména právo na respektování soukromého života a komunikace, právo na ochranu osobních údajů, svobodu podnikání, právo na vlastnictví a právo na účinnou právní ochranu a spravedlivý proces. Tato směrnice by měla být prováděna v souladu s těmito právy a zásadami,	(84) Tato směrnice dodržuje základní práva a ctí zásady uznané Listinou základních práv Evropské unie, zejména právo na respektování soukromého života a komunikace, právo na ochranu osobních údajů, svobodu podnikání, právo na vlastnictví a právo na účinnou právní ochranu a spravedlivý proces. Tato směrnice by měla být prováděna v souladu s těmito právy a zásadami ***a při plném dodržování stávajících právních předpisů Unie**, **které upravují tyto otázky. Veškeré zpracování osobních údajů podle této směrnice podléhá nařízení (EU) 2016/679 a směrnici 2002/58/ES v rámci jejich příslušných oblastí působnosti, včetně úkolů a pravomocí dozorových úřadů a orgánů dozoru příslušných pro monitorování souladu s těmito právními nástroji.***

Pozměňovací návrh 47

Návrh směrnice
Čl. 2 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. Tato směrnice se vztahuje na veřejné a soukromé subjekty druhu, který je v příloze I označován za základní a v příloze II za důležitý. Tato směrnice se nevztahuje na subjekty, které splňují definici mikropodniků a malých podniků	1. Tato směrnice se vztahuje na veřejné a soukromé subjekty druhu, který je v příloze I označován za základní a v příloze II za důležitý. Tato směrnice se nevztahuje na subjekty, které splňují definici mikropodniků a malých podniků

ve smyslu doporučení Komise 2003/361/ES[28].	ve smyslu doporučení Komise 2003/361/ES[28]. ***Ustanovení čl. 3 odst. 4 přílohy k doporučení Komise 2003/361/ES se nepoužije.***
[28] Doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků (Úř. věst. L 124, 20.5.2003, s. 36).	[28] Doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků (Úř. věst. L 124, 20.5.2003, s. 36).

Pozměňovací návrh 48

Návrh směrnice
Čl. 2 – odst. 2 – návětí

Znění navržené Komisí	*Pozměňovací návrh*
2. Tato směrnice se však vztahuje také na subjekty uvedené v přílohách I a II bez ohledu na jejich velikost, pokud:	2. Tato směrnice se však vztahuje také na subjekty uvedené v přílohách I a II bez ohledu na jejich velikost ***na základě posouzení rizik podle článku 18***, pokud:

Pozměňovací návrh 49

Návrh směrnice
Čl. 2 – odst. 2 – písm. c

Znění navržené Komisí	*Pozměňovací návrh*
c) je subjekt výhradním dodavatelem služeb ***v členském státě***;	c) je subjekt výhradním dodavatelem služeb ***na vnitrostátní nebo regionální úrovni***;

Pozměňovací návrh 50

Návrh směrnice
Čl. 2 – odst. 2 – písm. d

Znění navržené Komisí	*Pozměňovací návrh*
d) by ***možné*** narušení služby poskytované tímto subjektem mohlo mít vliv na veřejný pořádek, veřejnou bezpečnost nebo ochranu zdraví;	d) by narušení služby poskytované tímto subjektem mohlo mít vliv na veřejný pořádek, veřejnou bezpečnost nebo ochranu zdraví;

Pozměňovací návrh 51

Návrh směrnice
Čl. 2 – odst. 2 – písm. e

Znění navržené Komisí	*Pozměňovací návrh*
e) by ***možné*** narušení služby poskytované tímto subjektem mohlo vyvolat systémová rizika, zejména pro ta odvětví, kde by takové narušení mohlo mít přeshraniční dopad;	e) by narušení služby poskytované tímto subjektem mohlo vyvolat systémová rizika, zejména pro ta odvětví, kde by takové narušení mohlo mít přeshraniční dopad;

Pozměňovací návrh 52

Návrh směrnice
Čl. 2 – odst. 4 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	4a. Veškeré zpracování osobních údajů podle této směrnice musí být v souladu s nařízením (EU) 2016/679 a směrnicí 2002/58/ES a musí být omezeno na to, co je pro účely této směrnice nezbytně nutné a přiměřené.

Pozměňovací návrh 53

Návrh směrnice
Čl. 2 – odst. 5

Znění navržené Komisí	*Pozměňovací návrh*
5. Aniž je dotčen článek 346 Smlouvy o fungování EU, ***se*** informace, které jsou důvěrné podle unijních a vnitrostátních pravidel, jako jsou pravidla pro zachovávání důvěrnosti obchodních informací, vyměňují s Komisí a jinými příslušnými orgány pouze v případě, že je tato výměna nutná pro účely této směrnice. Vyměňované informace se omezí na informace, které jsou ***relevantní a přiměřené účelu*** této výměny. Při těchto výměnách informací se zachovává důvěrnost předmětných informací a jsou chráněny bezpečnost a obchodní zájmy	5. Aniž je dotčen článek 346 Smlouvy o fungování EU, informace, které jsou důvěrné podle unijních a vnitrostátních pravidel, jako jsou pravidla pro zachovávání důvěrnosti obchodních informací, ***se*** vyměňují s Komisí a jinými příslušnými orgány pouze v případě, že je tato výměna nutná pro účely této směrnice. Vyměňované informace se omezí na informace, které jsou ***nezbytné pro účel*** této výměny. Při těchto výměnách informací se zachovává důvěrnost předmětných informací a jsou chráněny bezpečnost a obchodní zájmy základních

základních nebo důležitých subjektů.	nebo důležitých subjektů.

Pozměňovací návrh 54

Návrh směrnice
Čl. 2 – odst. 6 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	6a. Komise do 31. prosince 2021 zveřejní legislativní návrh na zahrnutí orgánů, institucí a jiných subjektů Unie do celkového unijního rámce pro kybernetickou bezpečnost, aby tak byla pomocí soudržných a homogenních pravidel dosažena jednotná úroveň ochrany.

Pozměňovací návrh 55

Návrh směrnice
Čl. 4 – odst. 1 – bod 1 – písm. b

Znění navržené Komisí	*Pozměňovací návrh*
b) zařízení nebo skupina vzájemně propojených nebo souvisejících zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování digitálních dat;	b) zařízení nebo skupina vzájemně propojených nebo souvisejících zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování digitálních dat ***a která jsou integrována do informačního systému a využívána pro poskytování jejich zamýšlených služeb***;

Pozměňovací návrh 56

Návrh směrnice
Čl. 4 – odst. 1 – bod 4

Znění navržené Komisí	*Pozměňovací návrh*
4) „národní strategií kybernetické bezpečnosti“ soudržný rámec členského státu vymezující strategické cíle a priority v oblasti ***bezpečnosti sítí a informačních systémů*** v tomto členském státě;	4) „národní strategií kybernetické bezpečnosti“ soudržný rámec členského státu vymezující strategické cíle a priority v oblasti ***kybernetické bezpečnosti*** v tomto členském státě;

Pozměňovací návrh 57

Návrh směrnice
Čl. 4 – odst. 1 – bod 12

Znění navržené Komisí	*Pozměňovací návrh*
12) „výměnným uzlem internetu (IXP)“ síťové zařízení umožňující propojení více než dvou nezávislých sítí (autonomních systémů), a to primárně pro účely usnadnění výměny dat zasílaných prostřednictvím internetu; výměnný uzel internetu poskytuje propojení pouze autonomním systémům; výměnný uzel internetu nevyžaduje, aby data zasílaná prostřednictvím internetu mezi kterýmikoli dvěma zúčastněnými autonomními systémy procházela přes jakýkoli třetí autonomní systém, ani zasílaná data nemění ani žádným jiným způsobem do jejich zasílání nezasahuje;	***vypouští se***

Pozměňovací návrh 58

Návrh směrnice
Čl. 4 – odst. 1 – bod 22

Znění navržené Komisí	*Pozměňovací návrh*
22) „platformou sociálních sítí“ platforma, která koncovým uživatelům umožňuje vzájemné propojení, sdílení, objevování a komunikaci napříč různými zařízeními, zejména prostřednictvím chatů, příspěvků, videí a doporučení;	***vypouští se***

Pozměňovací návrh 59

Návrh směrnice
Čl. 4 – odst. 1 – bod 24

Znění navržené Komisí	*Pozměňovací návrh*
24) „subjektem“ jakákoli fyzická nebo právnická osoba vytvořená a uznaná jako taková podle vnitrostátních právních předpisů v místě svého usazení, která může	24) „subjektem“ jakákoli fyzická ***osoba*** nebo ***jakákoli*** právnická osoba vytvořená a uznaná jako taková podle vnitrostátních právních předpisů v místě svého usazení,

svým jménem vykonávat práva a podléhat povinnostem;	která může svým jménem vykonávat práva a podléhat povinnostem;

Pozměňovací návrh 60

Návrh směrnice
Čl. 5 – odst. 1 – písm. a

Znění navržené Komisí	*Pozměňovací návrh*
a) definici cílů a priorit strategie kybernetické bezpečnosti členských států;	a) definici cílů a priorit strategie kybernetické bezpečnosti členských států ***s ohledem na obecnou úroveň povědomí občanů o kybernetické bezpečnosti a na obecnou úroveň bezpečnosti připojených spotřebitelských zařízení***;

Pozměňovací návrh 61

Návrh směrnice
Čl. 5 – odst. 1 – písm. f

Znění navržené Komisí	*Pozměňovací návrh*
f) politický rámec pro lepší koordinaci mezi příslušnými orgány podle této směrnice a směrnice Evropského parlamentu a Rady (EU) XXXX/XXXX***[38]*** [směrnice o odolnosti kritických subjektů] pro účely sdílení informací o incidentech a kybernetických hrozbách pro výkon úkolů v oblasti dohledu.	f) politický rámec pro lepší koordinaci mezi příslušnými orgány podle této směrnice a směrnice Evropského parlamentu a Rady (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů]***, jak na vnitrostátní úrovni, tak i mezi členskými státy,*** pro účely sdílení informací o incidentech a kybernetických hrozbách pro výkon úkolů v oblasti dohledu.
[38] [vložte úplný název a údaje o vyhlášení v Úředním věstníku, až budou známy]	[38] [vložte úplný název a údaje o vyhlášení v Úředním věstníku, až budou známy]

Pozměňovací návrh 62

Návrh směrnice
Čl. 5 – odst. 2 – písm. b

Znění navržené Komisí	*Pozměňovací návrh*
b) pokyny týkající se zařazení a	b) pokyny týkající se zařazení a

specifikace požadavků na kybernetickou bezpečnost produktů a služeb IKT při zadávání veřejných zakázek;	specifikace požadavků na kybernetickou bezpečnost produktů a služeb IKT při zadávání veřejných zakázek***, mimo jiné požadavků na šifrování a podporu využívání produktů kybernetické bezpečnosti s otevřeným zdrojovým kódem***;

Pozměňovací návrh 63

Návrh směrnice
Čl. 5 – odst. 2 – písm. d a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	da) politiku podporující zachování používání veřejně přístupných dat a otevřených zdrojů v rámci koncepce „bezpečnost skrze transparentnost“;

Pozměňovací návrh 64

Návrh směrnice
Čl. 5 – odst. 2 – písm. d b (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	db) politiku podporující soukromí a bezpečnost osobních údajů uživatelů on-line služeb;

Pozměňovací návrh 65

Návrh směrnice
Čl. 5 – odst. 2 – písm. e

Znění navržené Komisí	*Pozměňovací návrh*
e) politiku za účelem prosazování a rozvíjení dovedností v oblasti kybernetické bezpečnosti, zvyšování informovanosti a výzkumných a vývojových iniciativ;	e) politiku za účelem prosazování a rozvíjení dovedností v oblasti kybernetické bezpečnosti, zvyšování informovanosti a výzkumných a vývojových iniciativ***, včetně vypracování programů odborné přípravy v oblasti kybernetické bezpečnosti, aby měly subjekty k dispozici odborníky a techniky***;

Pozměňovací návrh 66

Návrh směrnice
Čl. 5 – odst. 2 – písm. f

Znění navržené Komisí	*Pozměňovací návrh*
f) politiku za účelem podpory akademických a výzkumných institucí ***při vývoji*** nástrojů kybernetické bezpečnosti a zabezpečené síťové infrastruktury;	f) politiku za účelem podpory akademických a výzkumných institucí***, které přispívají k vnitrostátní strategii v oblasti kybernetické bezpečnosti vývojem a zaváděním*** nástrojů kybernetické bezpečnosti a zabezpečené síťové infrastruktury***, včetně konkrétních politik zaměřených na zastoupení žen a mužů a genderovou rovnováhu v tomto odvětví***;

Pozměňovací návrh 67

Návrh směrnice
Čl. 5 – odst. 2 – písm. h

Znění navržené Komisí	*Pozměňovací návrh*
h) politiku řešící zvláštní potřeby malých a středních podniků, zejména těch, které nespadají do oblasti působnosti této směrnice, v souvislosti s pokyny a podporou při zlepšování jejich odolnosti vůči kybernetickým hrozbám.	h) politiku řešící zvláštní potřeby malých a středních podniků, zejména těch, které nespadají do oblasti působnosti této směrnice, v souvislosti s pokyny a podporou při zlepšování jejich odolnosti vůči kybernetickým hrozbám ***a jejich schopnosti reagovat na kybernetické bezpečnostní incidenty***.

Pozměňovací návrh 68

Návrh směrnice
Čl. 6 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Agentura ENISA vytvoří a spravuje Evropský registr zranitelností. Za tímto účelem ENISA zřídí a spravuje informační systémy, politiky a postupy s cílem zejména umožnit důležitým a základním subjektům a jejich dodavatelům sítí a informačních systémů odhalovat a	2. Agentura ENISA vytvoří a spravuje Evropský registr zranitelností. Za tímto účelem ENISA zřídí a spravuje informační systémy, politiky a postupy s cílem zejména umožnit důležitým a základním subjektům a jejich dodavatelům sítí a informačních systémů odhalovat a

registrovat zranitelná místa v produktech nebo službách IKT a poskytovat přístup k informacím o těchto zranitelnostech uvedeným v registru všem zúčastněným stranám. V registru jsou zejména uvedeny informace popisující slabé místo, dotčený produkt IKT nebo služby IKT a závažnost této zranitelnosti z hlediska okolností, za nichž může být využita, dostupnost příslušných oprav, a pokud opravy nejsou dostupné, pokyny pro uživatele zranitelných produktů a služeb, jak mohou být rizika vyplývající z odhalených slabých míst zmírněna.	registrovat zranitelná místa v produktech nebo službách IKT a poskytovat přístup k informacím o těchto zranitelnostech uvedeným v registru všem zúčastněným stranám. V registru jsou zejména uvedeny informace popisující slabé místo, dotčený produkt IKT nebo služby IKT a závažnost této zranitelnosti z hlediska okolností, za nichž může být využita, dostupnost příslušných oprav, a pokud opravy nejsou dostupné, pokyny pro uživatele zranitelných produktů a služeb, jak mohou být rizika vyplývající z odhalených slabých míst zmírněna. ***V zájmu zajištění bezpečnosti a přístupnosti informací v registru zavede agentura ENISA nejmodernější bezpečnostní opatření a informace zpřístupní na odpovídajících rozhraních ve strojově čitelném formátu.***

Pozměňovací návrh 69

Návrh směrnice
Čl. 7 – odst. 3 – písm. a

Znění navržené Komisí	*Pozměňovací návrh*
a) cíle vnitrostátních opatření a činností v oblasti připravenosti;	a) cíle vnitrostátních ***a případně regionálních a přeshraničních*** opatření a činností v oblasti připravenosti;

Pozměňovací návrh 70

Návrh směrnice
Čl. 10 – odst. 2 – písm. e

Znění navržené Komisí	*Pozměňovací návrh*
e) provádění ***aktivního*** skenování ***sítě*** a informačních systémů používaných k poskytování služeb subjektu, který o to požádal;	e) provádění ***bezpečnostního*** skenování informačních systémů a ***rozsahu sítě*** používaných k poskytování služeb subjektu, který o to požádal***, s cílem identifikovat a zmírnit konkrétní hrozby nebo jim předejít***; ***zpracování osobních údajů v souvislosti s tímto skenováním se omezí na nezbytně nutné údaje, v každém***

	případě na IP adresy a internetové adresy (URL);

Pozměňovací návrh 71

Návrh směrnice
Čl. 11 – odst. 4

Znění navržené Komisí	*Pozměňovací návrh*
4. V rozsahu nezbytném pro účelné plnění úkolů a povinností stanovených touto směrnicí zajistí členské státy vhodnou spolupráci mezi příslušnými orgány a jednotnými kontaktními místy a donucovacími orgány, úřady pro ochranu osobních údajů a orgány odpovědnými za kritickou infrastrukturu podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] a vnitrostátními finančními orgány určenými v souladu s nařízením Evropského parlamentu a Rady (EU) XXXX/XXXX[39] [nařízení DORA] v daném členském státě.	4. V rozsahu nezbytném pro účelné plnění úkolů a povinností stanovených touto směrnicí zajistí členské státy vhodnou spolupráci mezi příslušnými orgány a jednotnými kontaktními místy a donucovacími orgány, úřady pro ochranu osobních údajů a orgány odpovědnými za kritickou infrastrukturu podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] a vnitrostátními finančními orgány určenými v souladu s nařízením Evropského parlamentu a Rady (EU) XXXX/XXXX[39] [nařízení DORA] v daném členském státě ***v souladu s jejich příslušnými pravomocemi***.
[39] [vložte úplný název a údaje o vyhlášení v Úředním věstníku, až budou známy]	[39] [vložte úplný název a údaje o vyhlášení v Úředním věstníku, až budou známy]

Pozměňovací návrh 72

Návrh směrnice
Čl. 11 – odst. 5

Znění navržené Komisí	*Pozměňovací návrh*
5. Členské státy zajistí, aby jejich příslušné orgány pravidelně poskytovaly informace příslušným orgánům určeným podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] o kybernetických bezpečnostních rizicích, kybernetických hrozbách a incidentech postihujících základní subjekty určené jako kritické nebo jako subjekty rovnocenné kritickým subjektům podle směrnice (EU)	5. Členské státy zajistí, aby jejich příslušné orgány pravidelně ***a včas*** poskytovaly informace příslušným orgánům určeným podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] o kybernetických bezpečnostních rizicích, kybernetických hrozbách a incidentech postihujících základní subjekty určené jako kritické nebo jako subjekty rovnocenné kritickým

XXXX/XXXX [směrnice o odolnosti kritických subjektů], jakož i o opatřeních, jež příslušné orgány přijaly v reakci na tato rizika a incidenty.	subjektům podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů], jakož i o opatřeních, jež příslušné orgány přijaly v reakci na tato rizika a incidenty.

Pozměňovací návrh 73

Návrh směrnice
Čl. 12 – odst. 3 – návětí

Znění navržené Komisí	*Pozměňovací návrh*
3. Skupina pro spolupráci je tvořena zástupci členských států, Komise a agentury ENISA. Činností skupiny pro spolupráci se jako pozorovatel účastní Evropská služba pro vnější činnost. Činností skupiny pro spolupráci se mohou účastnit evropské orgány dohledu v souladu s čl. 17 odst. 5 písm. c) nařízení (EU) XXXX/XXXX [nařízení DORA].	3. Skupina pro spolupráci je tvořena zástupci členských států, Komise a agentury ENISA. Činností skupiny pro spolupráci se jako pozorovatel účastní Evropská služba pro vnější činnost***, Evropské centrum pro boj proti kyberkriminalitě při Europolu a Evropský sbor pro ochranu osobních údajů***. Činností skupiny pro spolupráci se mohou účastnit evropské orgány dohledu v souladu s čl. 17 odst. 5 písm. c) nařízení (EU) XXXX/XXXX [nařízení DORA].

Pozměňovací návrh 74

Návrh směrnice
Čl. 12 – odst. 3 – pododstavec 1

Znění navržené Komisí	*Pozměňovací návrh*
Tam, kde je to vhodné, ***může*** skupina pro spolupráci ***přizvat*** ke spolupráci zástupce příslušných zúčastněných stran.	***Je-li to relevantní pro plnění jejích úkolů***, skupina pro spolupráci ***přizve*** ke spolupráci zástupce příslušných zúčastněných stran ***a dále Evropský parlament jako pozorovatele***.

Pozměňovací návrh 75

Návrh směrnice
Čl. 12 – odst. 8

Znění navržené Komisí	*Pozměňovací návrh*
8. Skupina pro spolupráci se schází pravidelně, alespoň ***jednou*** ročně, se skupinou pro odolnost kritických subjektů zřízenou podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] za účelem ***podpory*** strategické spolupráce a výměny informací.	8. Skupina pro spolupráci se schází pravidelně, alespoň ***dvakrát*** ročně, se skupinou pro odolnost kritických subjektů zřízenou podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] za účelem ***usnadnění*** strategické spolupráce a výměny informací ***v reálném čase***.

Pozměňovací návrh 76

Návrh směrnice
Čl. 13 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Síť CSIRT tvoří zástupci týmů CSIRT z členských států a týmu CERT–EU. Komise se účastní sítě CSIRT jako ***pozorovatel***. Agentura ENISA zajistí služby sekretariátu a aktivně podporuje spolupráci mezi týmy CSIRT.	2. Síť CSIRT tvoří zástupci týmů CSIRT z členských států a týmu CERT–EU. Komise ***a Evropské centrum pro boj proti kyberkriminalitě při Europolu*** se účastní sítě CSIRT jako ***pozorovatelé***. Agentura ENISA zajistí služby sekretariátu a aktivně podporuje spolupráci mezi týmy CSIRT.

Pozměňovací návrh 77

Návrh směrnice
Čl. 14 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Síť EU-CyCLONe je tvořena zástupci orgánů krizového řízení členských států určených podle článku 7, Komise a agentury ENISA. Agentura ENISA zajišťuje služby sekretariátu a podporuje bezpečnou výměnu informací.	2. Síť EU-CyCLONe je tvořena zástupci orgánů krizového řízení členských států určených podle článku 7, Komise a agentury ENISA. ***Evropské centrum pro boj proti kyberkriminalitě při Europolu se činností sítě EU-CyCLONe účastní jako pozorovatel.*** Agentura ENISA zajišťuje služby sekretariátu a podporuje bezpečnou výměnu informací.

Pozměňovací návrh 78

Návrh směrnice

Čl. 14 – odst. 6

Znění navržené Komisí	*Pozměňovací návrh*
6. Síť EU-CyCLONe spolupracuje se sítí CSIRT podle sjednaných procesních pravidel.	6. Síť EU-CyCLONe spolupracuje se sítí CSIRT podle sjednaných procesních pravidel ***a s donucovacími orgány v rámci protokolu EU o vymáhání práva v případě nouze***.

Pozměňovací návrh 79

Návrh směrnice
Čl. 15 – odst. 1 – návětí

Znění navržené Komisí	*Pozměňovací návrh*
1. Agentura ENISA ve spolupráci s Komisí vydává jednou ***za dva roky*** zprávu o stavu kybernetické bezpečnosti v Unii. Ve zprávě uvede zejména posouzení:	1. Agentura ENISA ve spolupráci s Komisí vydává jednou ***ročně*** zprávu o stavu kybernetické bezpečnosti v Unii. Ve zprávě***, kterou dodá ve strojově čitelném formátu,*** uvede zejména posouzení:

Pozměňovací návrh 80

Návrh směrnice
Čl. 15 – odst. 1 – písm. c a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	ca) dopadu kybernetických bezpečnostních incidentů na ochranu osobních údajů v Unii.

Pozměňovací návrh 81

Návrh směrnice
Čl. 15 – odst. 1 – písm. c b (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	cb) přehled obecné úrovně povědomí o kybernetické bezpečnosti a jejího používání mezi občany, jakož i obecné úrovně bezpečnosti připojených spotřebitelských zařízení, která jsou v Unii

uváděna na trh.

Pozměňovací návrh 82

Návrh směrnice
Čl. 17 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Členské státy zajistí, aby členové vedoucího orgánu pravidelně absolvovali zvláštní školení, a získali tak dostatečné znalosti a dovednosti, aby mohli posoudit a vyhodnotit kybernetická bezpečnostní rizika a řídicí postupy a jejich dopad na provoz subjektu.	2. Členské státy zajistí, aby členové vedoucího orgánu ***a pověření odborníci na kybernetickou bezpečnost*** pravidelně absolvovali zvláštní školení, a získali tak dostatečné znalosti a dovednosti, aby mohli posoudit a vyhodnotit kybernetická bezpečnostní rizika a řídicí postupy a jejich dopad na provoz subjektu.

Pozměňovací návrh 83

Návrh směrnice
Čl. 18 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. Členské státy zajistí, aby základní a důležité subjekty přijaly vhodná a přiměřená technická a organizační opatření k řízení ***bezpečnostních*** rizik***, jimž čelí*** sítě a ***informační systémy***, jež tyto subjekty používají pro poskytování svých služeb. S ohledem na nejnovější technický vývoj musí tato opatření zajišťovat úroveň bezpečnosti sítí a informačních systémů odpovídající existující míře rizika.	1. Členské státy zajistí, aby základní a důležité subjekty přijaly vhodná a přiměřená technická a organizační opatření k řízení rizik ***pro kybernetickou bezpečnost*** sítě a ***informačních systémů***, jež tyto subjekty používají pro poskytování svých služeb***, a k zajištění kontinuity těchto služeb a zmírnění rizik pro práva jednotlivců při zpracování jejich osobních údajů***. S ohledem na nejnovější technický vývoj musí tato opatření zajišťovat úroveň ***kybernetické*** bezpečnosti sítí a informačních systémů odpovídající existující míře rizika.

Pozměňovací návrh 84

Návrh směrnice
Čl. 18 – odst. 2 – písm. g

Znění navržené Komisí	*Pozměňovací návrh*

g) používání kryptografie a šifrování.	g) používání kryptografie a silného šifrování.

Pozměňovací návrh 85

Návrh směrnice
Čl. 18 – odst. 3

Znění navržené Komisí	*Pozměňovací návrh*
3. Členské státy zajistí, aby při zvažování vhodných opatření uvedených v odst. 2 písm. d) subjekty zohlednily zranitelnosti specifické pro každého dodavatele a poskytovatele služeb a celkovou kvalitu produktů a praktik v oblasti kybernetické bezpečnosti svých dodavatelů a poskytovatelů služeb, včetně jejich postupů bezpečného vývoje.	3. Členské státy zajistí, aby při zvažování vhodných ***a přiměřených*** opatření uvedených v odst. 2 písm. d) subjekty zohlednily zranitelnosti specifické pro každého dodavatele a poskytovatele služeb a celkovou kvalitu produktů a praktik v oblasti kybernetické bezpečnosti svých dodavatelů a poskytovatelů služeb, včetně jejich postupů bezpečného vývoje. ***Příslušné orgány poskytují subjektům pokyny pro praktické a přiměřené uplatňování těchto opatření.***

Pozměňovací návrh 86

Návrh směrnice
Čl. 18 – odst. 6 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	6a. Členské státy přiznají uživateli sítě a informačního systému poskytovaného základním nebo významným subjektem právo získat od tohoto subjektu informace o zavedených technických a organizačních opatřeních k řízení rizik pro bezpečnost sítí a informačních systémů. Členské státy stanoví omezení tohoto práva.

Pozměňovací návrh 87

Návrh směrnice
Čl. 19 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. Skupina pro spolupráci ***může v***	1. Skupina pro spolupráci ***provede ve***

součinnosti s Komisí a agenturou ENISA ***provést*** koordinované posouzení rizik dodavatelských řetězců u specifických kritických služeb, systémů nebo produktů IKT, přičemž zohlední technické, případně netechnické rizikové faktory.

spolupráci s Komisí a agenturou ENISA koordinované posouzení rizik dodavatelských řetězců u specifických kritických služeb, systémů nebo produktů IKT, přičemž zohlední technické, případně netechnické rizikové faktory.

Pozměňovací návrh 88

Návrh směrnice
Čl. 20 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. Členské státy zajistí, aby základní a důležité subjekty neprodleně oznamovaly příslušným orgánům nebo týmu CSIRT v souladu s odstavci 3 a 4 každý incident, který má závažný dopad na poskytování jejich služeb***. Ve vhodných případech*** tyto subjekty neprodleně informují příjemce svých služeb o incidentech, které by mohly negativně ovlivnit poskytování dané služby. Členské státy zajistí, aby tyto subjekty oznamovaly mimo jiné všechny informace, které příslušným orgánům nebo týmu CSIRT umožní posoudit případný přeshraniční dopad daného incidentu.	1. Členské státy zajistí, aby základní a důležité subjekty neprodleně***, nejpozději však do 24 hodin,*** oznamovaly příslušným orgánům nebo týmu CSIRT v souladu s odstavci 3 a 4 každý incident, který má závažný dopad na poskytování jejich služeb***, a pokud by incident mohl mít nebo má škodlivou povahu, aby jej oznámily příslušným donucovacím orgánům.*** Tyto subjekty neprodleně***, nejpozději však do 24 hodin,*** informují příjemce svých služeb o incidentech, které by mohly negativně ovlivnit poskytování dané služby***, a poskytnou jim informace, které jim umožní zmírnit nepříznivé dopady kybernetických útoků. Ve výjimečných případech, kdy by zveřejnění mohlo vyvolat další kybernetické útoky, by zásadní a důležité subjekty mohly oznámení odložit***. Členské státy zajistí, aby tyto subjekty oznamovaly mimo jiné všechny informace, které příslušným orgánům nebo týmu CSIRT umožní posoudit případný přeshraniční dopad daného incidentu.

Pozměňovací návrh 89

Návrh směrnice
Čl. 20 – odst. 2 – návětí

Znění navržené Komisí	*Pozměňovací návrh*
2. Členské státy zajistí, aby základní a důležité subjekty ***neprodleně oznamovaly*** příslušným orgánům nebo týmu CSIRT každou významnou kybernetickou hrozbu, kterou tyto subjekty zjistí a která by mohla mít za následek významný incident.	2. Členské státy zajistí, aby základní a důležité subjekty ***mohly*** příslušným orgánům nebo týmu CSIRT ***oznámit*** každou významnou kybernetickou hrozbu, kterou tyto subjekty zjistí a která by mohla mít za následek významný incident.

Pozměňovací návrh 90

Návrh směrnice
Čl. 20 – odst. 2 – pododstavec 1

Znění navržené Komisí	*Pozměňovací návrh*
Ve vhodných případech tyto subjekty ***neprodleně informují*** příjemce svých služeb, které mohou být ovlivněny významnou kybernetickou hrozbou, o všech krocích nebo nápravných opatřeních, jež příjemci mohou učinit v reakci na danou hrozbu. ***Ve vhodných případech subjekty příjemce*** uvědomí také o hrozbě samotné. Ohlášení nezakládá u oznamujícího subjektu vyšší míru právní odpovědnosti.	Ve vhodných případech ***mohou*** tyto subjekty ***informovat*** příjemce svých služeb, které mohou být ovlivněny významnou kybernetickou hrozbou, o všech krocích nebo nápravných opatřeních, jež příjemci mohou učinit v reakci na danou hrozbu. ***Pokud tyto subjekty učiní takové ohlášení,*** uvědomí ***příjemce*** také o hrozbě samotné. Ohlášení nezakládá u oznamujícího subjektu vyšší míru právní odpovědnosti.

Pozměňovací návrh 91

Návrh směrnice
Čl. 20 – odst. 4 – písm. c – návětí

Znění navržené Komisí	*Pozměňovací návrh*
c) nejpozději do jednoho měsíce od předložení oznámení podle písmene a) ***závěrečnou*** zprávu zahrnující alespoň:	c) nejpozději do jednoho měsíce od předložení oznámení podle písmene a) ***komplexní*** zprávu zahrnující alespoň:

Pozměňovací návrh 92

Návrh směrnice
Čl. 20 – odst. 4 – písm. c – bod ii

Znění navržené Komisí	*Pozměňovací návrh*
ii) druh hrozby nebo základní příčinu, která incident pravděpodobně spustila;	ii) druh ***kybernetické*** hrozby nebo základní příčinu, která incident pravděpodobně spustila;

Pozměňovací návrh 93

Návrh směrnice
Čl. 20 – odst. 4 – písm. c – bod iii

Znění navržené Komisí	*Pozměňovací návrh*
iii) učiněná a probíhající opatření ke zmírnění následků.	iii) učiněná a probíhající opatření ke zmírnění následků ***nebo nápravná opatření***.

Pozměňovací návrh 94

Návrh směrnice
Čl. 20 – odst. 6

Znění navržené Komisí	*Pozměňovací návrh*
6. Tam, kde je to vhodné, a zejména pokud se incident podle odstavce 1 týká dvou nebo více členských států, informuje příslušný orgán nebo tým CSIRT, jimž byl incident ohlášen, ostatní dotčené členské státy a agenturu ENISA. Příslušné orgány, týmy CSIRT a jednotná kontaktní místa přitom v souladu s právem Unie nebo vnitrostátními právními předpisy, které jsou v souladu s právem Unie, zachovávají bezpečnost a obchodní zájmy subjektu, jakož i důvěrnost poskytnutých informací.	6. Tam, kde je to vhodné, a zejména pokud se incident podle odstavce 1 týká dvou nebo více členských států, informuje příslušný orgán nebo tým CSIRT, jimž byl incident ohlášen, ostatní dotčené členské státy a agenturu ENISA. ***Pokud se incident týká dvou nebo více členských států a existuje podezření, že má trestní povahu, příslušný orgán nebo tým CSIRT informuje EUROPOL.*** Příslušné orgány, týmy CSIRT a jednotná kontaktní místa přitom v souladu s právem Unie nebo vnitrostátními právními předpisy, které jsou v souladu s právem Unie, zachovávají bezpečnost a obchodní zájmy subjektu, jakož i důvěrnost poskytnutých informací.

Pozměňovací návrh 95

Návrh směrnice
Čl. 22 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Agentura ENISA ve spolupráci ***se*** členskými státy vydá doporučení a pokyny týkající se technických oblastí, které by měly být zohledněny ve vztahu k odstavci 1, jakož i s ohledem na již existující normy, včetně vnitrostátních norem členských států, které by umožnily tyto oblasti pokrýt.	2. Agentura ENISA ***po konzultaci s Evropským sborem pro ochranu osobních údajů a*** ve spolupráci ***s*** členskými státy vydá doporučení a pokyny týkající se technických oblastí, které by měly být zohledněny ve vztahu k odstavci 1, jakož i s ohledem na již existující normy, včetně vnitrostátních norem členských států, které by umožnily tyto oblasti pokrýt.

Pozměňovací návrh 96

Návrh směrnice
Čl. 23 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. Aby členské státy přispěly k bezpečnosti, stabilitě a odolnosti DNS, zajistí, aby ***registry*** TLD ***a subjekty poskytující služby registrace doménových jmen pro TLD shromažďovaly*** a ***uchovávaly přesné*** a ***úplné údaje*** o registraci doménových jmen ve vyhrazeném databázovém zařízení***, a to*** s ***náležitou péčí podle právních předpisů*** Unie o ochraně osobních údajů, pokud jde o data, jež jsou osobními údaji.	1. Aby členské státy přispěly k bezpečnosti, stabilitě a odolnosti DNS, zajistí, aby TLD ***měly zavedeny politiky a postupy, které zaručí shromažďování*** a ***uchovávání přesných*** a ***úplných údajů*** o registraci doménových jmen ve vyhrazeném databázovém zařízení ***v souladu*** s ***právními předpisy*** Unie o ochraně osobních údajů, pokud jde o data, jež jsou osobními údaji. ***Členské státy zajistí, aby tyto politiky a postupy byly veřejně přístupné.***

Pozměňovací návrh 97

Návrh směrnice
Čl. 23 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Členské státy zajistí, aby databáze údajů o registraci doménových jmen uvedené v odstavci 1 obsahovaly ***podstatné*** informace umožňující identifikaci a kontaktování držitelů doménových jmen a	2. Členské státy zajistí, aby databáze údajů o registraci doménových jmen uvedené v odstavci 1 obsahovaly ***nezbytné*** informace umožňující identifikaci a kontaktování držitelů doménových jmen**,**

kontaktní místa spravující doménová jména v registrech TLD.	***konkrétně jejich jméno, poštovní*** a ***e-mailovou adresu a telefonní číslo,*** ***a*** kontaktní místa spravující doménová jména v registrech TLD.

Pozměňovací návrh 98

Návrh směrnice
Čl. 23 – odst. 3

Znění navržené Komisí	*Pozměňovací návrh*
3. Členské státy zajistí, aby registry TLD a subjekty poskytující služby registrace doménových jmen pro TLD měly zavedeny zásady a postupy zajišťující, aby databáze zahrnovaly přesné a úplné informace. Členské státy zajistí, aby byly tyto zásady a postupy veřejně dostupné.	***vypouští se***

Odůvodnění

Tento odstavec byl zařazen do čl. 23 odst. 1.

Pozměňovací návrh 99

Návrh směrnice
Čl. 23 – odst. 4

Znění navržené Komisí	*Pozměňovací návrh*
4. Členské státy zajistí, aby registry TLD a subjekty poskytující služby registrace doménových jmen pro TLD ***zveřejnily*** neprodleně po registraci doménového jména údaje o registraci ***domény***, ***které nejsou osobními údaji***.	4. Členské státy zajistí, aby registry TLD a subjekty poskytující služby registrace doménových jmen pro TLD neprodleně po registraci doménového jména ***zveřejnily v souladu s čl. 6 odst. 1 písm. c) a čl. 6 odst. 3 nařízení (EU) 2016/679 určité*** údaje o registraci ***doménového jména***, ***jako je doménové jméno a název právnické osoby***.

Pozměňovací návrh 100

Návrh směrnice
Čl. 23 – odst. 5

Znění navržené Komisí	*Pozměňovací návrh*
5. Členské státy zajistí, aby registry TLD a subjekty poskytující služby registrace doménových jmen pro TLD poskytovaly přístup ke konkrétním údajům o registraci doménových jmen na oprávněnou a řádně odůvodněnou žádost ***oprávněných žadatelů o přístup***, a to v souladu s právními předpisy Unie o ochraně osobních údajů. Členské státy zajistí, aby registry TLD a subjekty poskytující služby registrace doménových jmen pro TLD neprodleně reagovaly na všechny žádosti o přístup. Členské státy zajistí, aby byly zásady a postupy zveřejňování těchto údajů veřejně dostupné.	5. Členské státy zajistí, aby registry TLD a subjekty poskytující služby registrace doménových jmen pro TLD poskytovaly přístup ke konkrétním údajům o registraci doménových jmen na oprávněnou a řádně odůvodněnou žádost ***orgánů veřejné správy, včetně příslušných orgánů podle této směrnice, příslušných orgánů podle unijního nebo vnitrostátního práva pro prevenci, vyšetřování či stíhání trestných činů nebo dozorových úřadů podle nařízení (EU) 2016/679***, a to v souladu s právními předpisy Unie o ochraně osobních údajů. Členské státy zajistí, aby registry TLD a subjekty poskytující služby registrace doménových jmen pro TLD neprodleně reagovaly na všechny ***zákonné a řádně zdůvodněné*** žádosti o přístup. Členské státy zajistí, aby byly zásady a postupy zveřejňování těchto údajů veřejně dostupné.

Pozměňovací návrh 101

Návrh směrnice
Čl. 24 – odst. 3

Znění navržené Komisí	*Pozměňovací návrh*
3. Jestliže subjekt uvedený v odstavci 1 není v Unii usazen, ale nabízí v Unii služby, určí svého zástupce v Unii. Tento zástupce musí být usazen v jednom z členských států, v němž jsou služby nabízeny. Má se za to, že tento subjekt podléhá pravomoci členského státu, v němž je zástupce usazen. Neexistuje-li určený zástupce v Unii podle tohoto článku, může právní kroky proti subjektu za neplnění povinností podle této směrnice	3. Jestliže subjekt uvedený v odstavci 1 není v Unii usazen, ale nabízí v Unii služby, určí svého zástupce v Unii. Tento zástupce musí být usazen v jednom z členských států, v němž jsou služby nabízeny. ***Aniž jsou dotčeny pravomoci dozorových úřadů podle nařízení (EU) 2016/679,*** má se za to, že tento subjekt podléhá pravomoci členského státu, v němž je zástupce usazen. Neexistuje-li určený zástupce v Unii podle tohoto

podniknout kterýkoli členský stát, v němž tento subjekt poskytuje služby.	článku, může právní kroky proti subjektu za neplnění povinností podle této směrnice podniknout kterýkoli členský stát, v němž tento subjekt poskytuje služby.

Pozměňovací návrh 102

Návrh směrnice
Čl. 25 – odst. 1 – návětí

Znění navržené Komisí	*Pozměňovací návrh*
1. Agentura ENISA vytvoří a vede registr základních a důležitých subjektů uvedených v čl. 24 odst. 1. Subjekty předloží [nejpozději do 12 měsíců od vstupu této směrnice v platnost] agentuře ENISA tyto informace:	1. Agentura ENISA vytvoří a vede ***zabezpečený*** registr základních a důležitých subjektů uvedených v čl. 24 odst. 1. Subjekty předloží [nejpozději do 12 měsíců od vstupu této směrnice v platnost] agentuře ENISA tyto informace:

Pozměňovací návrh 103

Návrh směrnice
Čl. 26 – odst. 1 – návětí

Znění navržené Komisí	*Pozměňovací návrh*
1. Aniž je dotčeno nařízení (EU) 2016/679 členské státy zajistí, aby základní a důležité subjekty mohly mezi sebou sdílet podstatné informace o kybernetické bezpečnosti včetně informací týkajících se kybernetických hrozeb, zranitelností, indikátorů narušení, taktiky, technik a postupů, varování při ohrožení kybernetické bezpečnosti a konfiguračních nástrojů, pokud toto sdílení informací:	1. Aniž je dotčeno nařízení (EU) 2016/679 ***nebo směrnice 2002/58/ES,*** členské státy zajistí, aby základní a důležité subjekty mohly mezi sebou sdílet podstatné informace o kybernetické bezpečnosti včetně informací týkajících se kybernetických hrozeb, zranitelností, indikátorů narušení, taktiky, technik a postupů, varování při ohrožení kybernetické bezpečnosti a konfiguračních nástrojů ***a poloze nebo totožnosti útočníka***, pokud toto sdílení informací:

Pozměňovací návrh 104

Návrh směrnice
Čl. 28 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Při řešení incidentů, v jejichž	2. Při řešení incidentů, v jejichž

důsledku došlo k porušení ochrany osobních údajů, příslušné orgány úzce spolupracují s orgány pro ***ochranu*** osobních údajů.	důsledku došlo k porušení ochrany osobních údajů, příslušné orgány úzce spolupracují s orgány ***dohledu, aniž jsou dotčeny kompetence, úkoly a pravomoci dozorových úřadů podle nařízení (EU) 2016/679. Za tímto účelem si příslušné orgány a orgány dohledu vyměňují informace relevantní pro jejich příslušnou oblast působnosti. Kromě toho příslušné orgány na žádost příslušných orgánů dohledu poskytnou veškeré informace získané v rámci auditů a šetření, které se týkají zpracování osobních údajů.***

Pozměňovací návrh 105

Návrh směrnice
Čl. 29 – odst. 4 – písm. h

Znění navržené Komisí	*Pozměňovací návrh*
h) nařídit těmto subjektům, aby konkrétním způsobem zveřejnily aspekty nedodržování povinností stanovených v této směrnici;	***vypouští se***

Pozměňovací návrh 106

Návrh směrnice
Čl. 29 – odst. 5 – písm. b

Znění navržené Komisí	*Pozměňovací návrh*
b) uložit nebo požadovat, aby příslušné orgány nebo soudy v souladu s vnitrostátními právními předpisy uložily dočasný zákaz výkonu manažerských funkcí v tomto subjektu jakékoli osobě, která má manažerskou odpovědnost na úrovni výkonného ředitele nebo zákonného zástupce v tomto základním subjektu, i jakékoli jiné fyzické osobě odpovědné za porušení.	***vypouští se***

Pozměňovací návrh 107

Návrh směrnice
Čl. 29 – odst. 5 – pododstavec 1

Znění navržené Komisí	*Pozměňovací návrh*
Tato omezující opatření se ***použijí*** pouze do doby, než subjekt přijme opatření nezbytná k odstranění nedostatků nebo splnění požadavků příslušného orgánu, kvůli nimž ***byla tato*** omezující opatření ***uplatněna***.	***Toto*** omezující opatření se ***použije*** pouze do doby, než subjekt přijme opatření nezbytná k odstranění nedostatků nebo splnění požadavků příslušného orgánu, kvůli nimž ***bylo toto*** omezující opatření ***uplatněno***.

Pozměňovací návrh 108

Návrh směrnice
Čl. 29 – odst. 7 – písm. c

Znění navržené Komisí	*Pozměňovací návrh*
c) skutečně ***způsobené škody*** nebo ***vzniklé ztráty, případně potenciální*** škody nebo ***ztráty, které mohly být způsobeny***, pokud je lze určit. Při hodnocení tohoto aspektu je třeba zohlednit mimo jiné skutečné nebo potenciální finanční nebo ekonomické ztráty, účinky na jiné služby, počet postižených nebo potenciálně postižených uživatelů;	c) skutečně ***hmotné*** nebo ***nehmotné*** škody nebo ***vzniklé ztráty***, pokud je lze určit. Při hodnocení tohoto aspektu je třeba zohlednit mimo jiné skutečné nebo potenciální finanční nebo ekonomické ztráty, účinky na jiné služby, počet postižených nebo potenciálně postižených uživatelů;

Pozměňovací návrh 109

Návrh směrnice
Čl. 29 – odst. 7 – písm. c a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	ca) veškerá relevantní porušení, kterých se dotyčný subjekt dopustil v minulosti;

Pozměňovací návrh 110

Návrh směrnice
Čl. 29 – odst. 7 – písm. c b (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	cb) způsob, jakým se příslušný orgán dozvěděl o porušení, zejména zda a případně v jaké míře porušení oznámil subjekt;

Pozměňovací návrh 111

Návrh směrnice
Čl. 29 – odst. 7 – písm. g

Znění navržené Komisí	*Pozměňovací návrh*
g) míru spolupráce ***fyzické nebo právnické osoby považované za odpovědnou*** s příslušnými orgány**.**	g) míru spolupráce s příslušnými orgány ***za účelem nápravy porušení a zmírnění jeho možných nežádoucích účinků;***

Pozměňovací návrh 112

Návrh směrnice
Čl. 29 – odst. 7 – písm. g a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	ga) jakoukoliv jinou přitěžující nebo polehčující okolnost daného případu, např. získaný finanční prospěch či zamezené ztráty přímo či nepřímo vyplývající z porušení.

Pozměňovací návrh 113

Návrh směrnice
Čl. 29 – odst. 9

Znění navržené Komisí	*Pozměňovací návrh*
9. Členské státy zajistí, aby jejich příslušné orgány při výkonu svých pravomocí v oblasti dohledu a vymáhání zaměřených na zajištění dodržování povinností podle této směrnice ze strany základního subjektu určeného podle	9. Členské státy zajistí, aby jejich příslušné orgány při výkonu svých pravomocí v oblasti dohledu a vymáhání zaměřených na zajištění dodržování povinností podle této směrnice ze strany základního subjektu určeného podle

směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] za kritický subjekt nebo subjekt, který je rovnocenný kritickému subjektu, informovaly příslušné orgány ***daného členského státu určené*** podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů]. Na žádost příslušných orgánů podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] mohou příslušné orgány vykonávat své dohledové a donucovací pravomoci u základního subjektu označeného jako kritický nebo rovnocenný kritickému subjektu.

směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] za kritický subjekt nebo subjekt, který je rovnocenný kritickému subjektu, informovaly ***v reálném čase*** příslušné orgány ***všech členských států určených*** podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů]. Na žádost příslušných orgánů podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] mohou příslušné orgány vykonávat své dohledové a donucovací pravomoci u základního subjektu označeného jako kritický nebo rovnocenný kritickému subjektu.

Pozměňovací návrh 114

Návrh směrnice
Čl. 30 – odst. 4 – písm. g

Znění navržené Komisí	*Pozměňovací návrh*
g) nařídit těmto subjektům, aby konkrétním způsobem zveřejnily aspekty nedodržování jejich povinností stanovených v této směrnici;	***vypouští se***

Pozměňovací návrh 115

Návrh směrnice
Čl. 30 – odst. 4 – písm. h

Znění navržené Komisí	*Pozměňovací návrh*
h) učinit veřejné prohlášení, které identifikuje právnické ***a fyzické*** osoby odpovědné za porušení povinnosti stanovené v této směrnici a povahu tohoto porušení;	h) učinit veřejné prohlášení, které identifikuje právnické osoby odpovědné za porušení povinnosti stanovené v této směrnici a povahu tohoto porušení;

Pozměňovací návrh 116

Návrh směrnice
Čl. 31 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Správní pokuty se ukládají ***podle okolností každého jednotlivého případu kromě opatření uvedených*** v čl. 29 odst. 4 písm. a) až i), čl. 29 odst. 5 a čl. 30 odst. 4 písm. a) až h) či místo nich.	2. Správní pokuty se ukládají ***navíc k opatřením uvedeným*** v čl. 29 odst. 4 písm. a) až i), čl. 29 odst. 5 a čl. 30 odst. 4 písm. a) až h) či místo nich ***podle okolností každého jednotlivého případu***.

Pozměňovací návrh 117

Návrh směrnice
Čl. 31 – odst. 3

Znění navržené Komisí	*Pozměňovací návrh*
3. ***Při rozhodování*** o uložení správní pokuty a při rozhodování o její výši se v každém jednotlivém případě náležitě přihlédne alespoň k prvkům uvedeným v čl. 29 odst. 7.	3. ***Rozhodování*** o uložení správní pokuty ***závisí na okolnostech každého jednotlivého případu*** a při rozhodování o její výši se v každém jednotlivém případě náležitě přihlédne alespoň k prvkům uvedeným v čl. 29 odst. 7.

Pozměňovací návrh 118

Návrh směrnice
Čl. 32 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. Pokud mají příslušné orgány informace naznačující, že porušení povinností stanovených v článcích 18 a 20 základním nebo důležitým subjektem má za následek porušení zabezpečení osobních údajů ve smyslu čl. 4 odst. 12 nařízení (EU) 2016/679, které musí být oznámeno podle článku 33 uvedeného nařízení, uvědomí v ***přiměřené lhůtě orgány dohledu*** příslušné podle článků 55 a 56 uvedeného nařízení.	1. Pokud mají příslušné orgány informace naznačující, že porušení povinností stanovených v článcích 18 a 20 základním nebo důležitým subjektem má za následek porušení zabezpečení osobních údajů ve smyslu čl. 4 odst. 12 nařízení (EU) 2016/679, které musí být oznámeno podle článku 33 uvedeného nařízení, uvědomí ***neprodleně a*** v ***každém případě do 24 hodin dozorové úřady*** příslušné podle článků 55 a 56 uvedeného nařízení.

Pozměňovací návrh 119

Návrh směrnice
Čl. 32 – odst. 3

Znění navržené Komisí	*Pozměňovací návrh*
3. Pokud má dozorový úřad příslušný podle nařízení (EU) 2016/679 sídlo v jiném členském státě než příslušný orgán, ***může*** příslušný orgán ***informovat*** dozorový úřad se sídlem ve stejném členském státě.	3. Pokud má dozorový úřad příslušný podle nařízení (EU) 2016/679 sídlo v jiném členském státě než příslušný orgán, ***informuje*** příslušný orgán dozorový úřad se sídlem ve stejném členském státě.

Pozměňovací návrh 120

Návrh směrnice
Článek 34 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	Článek 34a
	Odpovědnost za nedodržení směrnice
	Aniž jsou dotčeny dostupné správní nebo mimosoudní opravné prostředky, mají příjemci služeb poskytovaných základními a důležitými subjekty, kterým vznikla škoda v důsledku nedodržení této směrnice ze strany poskytovatelů, právo na účinnou soudní ochranu.

Pozměňovací návrh 121

Návrh směrnice
Čl. 35 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
Komise ***pravidelně*** přezkoumává fungování této směrnice a podává zprávu Evropskému parlamentu a Radě. Ve zprávě ***se*** zejména posoudí význam odvětví, pododvětví, velikosti a druhu subjektů uvedených v přílohách I a II pro fungování hospodářství a společnosti v souvislosti s kybernetickou bezpečností. Za tímto účelem a s cílem dále rozvíjet strategickou a operativní spolupráci Komise zohlední zprávy skupiny pro spolupráci a sítě CSIRT z hlediska zkušeností získaných na strategické a operativní úrovni. První zprávu předloží do ... ***54*** měsíců od data vstupu této směrnice v platnost.	Komise přezkoumává fungování této směrnice ***každé tři roky*** a podává zprávu Evropskému parlamentu a Radě. Ve zprávě zejména posoudí***, do jaké míry směrnice přispívá k zajištění vysoké úrovně bezpečnosti a integrity sítě a informačních systémů a současně zajišťuje optimální ochranu soukromého života a osobních údajů, a*** význam odvětví, pododvětví, velikosti a druhu subjektů uvedených v přílohách I a II pro fungování hospodářství a společnosti v souvislosti s kybernetickou bezpečností. Za tímto účelem a s cílem dále rozvíjet strategickou a operativní spolupráci Komise zohlední zprávy skupiny pro spolupráci a sítě CSIRT z

hlediska zkušeností získaných na strategické a operativní úrovni. První zprávu předloží do ... □***36*** měsíců od data vstupu této směrnice v platnost□.

Pozměňovací návrh 122

Návrh směrnice
Příloha I – bod 5 (Zdravotnictví) – odrážka 6 (nová)

Znění navržené Komisí

Odvětví	Pododvětví	Druh subjektu
5. Zdravotnictví		– poskytovatelé zdravotní péče ve smyslu čl. 3 písm. g) směrnice 2011/24/EU (90) – referenční laboratoře EU ve smyslu článku 15 nařízení XXXX/XXXX o vážných přeshraničních zdravotních hrozbách[91] – subjekty provádějící výzkum a vývoj týkající se léčivých přípravků ve smyslu čl. 1 bodu 2 směrnice 2001/83/ES ([92]) – subjekty vyrábějící základní farmaceutické výrobky a farmaceutické přípravky ve smyslu sekce C oddílu 21 klasifikace NACE Rev. 2 – subjekty vyrábějící zdravotnické prostředky považované za kritické v případě ohrožení veřejného zdraví (uvedené na „seznamu kritických zdravotnických prostředků při mimořádné situaci v oblasti veřejného zdraví“) ve smyslu článku 20 nařízení XXXX[93]

[91] [Nařízení Evropského parlamentu a Rady o vážných přeshraničních zdravotních hrozbách a o zrušení rozhodnutí č. 1082/2013/EU, odkaz bude aktualizován, jakmile bude návrh COM(2020) 727 final přijat].

[92]Směrnice Evropského parlamentu a Rady 2001/83/ES ze dne 6. listopadu 2001 o kodexu Společenství týkajícím se humánních léčivých přípravků (Úř. věst. L 311, 28.11.2001, s. 67).

[93] [Nařízení Evropského parlamentu a Rady o posílené úloze Evropské agentury pro léčivé přípravky při připravenosti na krize a krizovém řízení v oblasti léčivých přípravků a zdravotnických prostředků, odkaz bude aktualizován, jakmile bude návrh COM(2020) 725 final přijat].

Pozměňovací návrh

Odvětví	Pododvětví	Druh subjektu
5. Zdravotnictví		– poskytovatelé zdravotní péče ve smyslu čl. 3 písm. g) směrnice 2011/24/EU (90)

– referenční laboratoře EU ve smyslu článku 15 nařízení XXXX/XXXX o vážných přeshraničních zdravotních hrozbách[91]

– subjekty provádějící výzkum a vývoj týkající se léčivých přípravků ve smyslu čl. 1 bodu 2 směrnice 2001/83/ES ([92])

– subjekty vyrábějící základní farmaceutické výrobky a farmaceutické přípravky ve smyslu sekce C oddílu 21 klasifikace NACE Rev. 2

– subjekty vyrábějící zdravotnické prostředky považované za kritické v případě ohrožení veřejného zdraví (uvedené na „seznamu kritických zdravotnických prostředků při mimořádné situaci v oblasti veřejného zdraví“) ve smyslu článku 20 nařízení XXXX[93]

– subjekty, které jsou držiteli povolení distribuce podle článku 79 směrnice 2001/83/ES

[91] [Nařízení Evropského parlamentu a Rady o vážných přeshraničních zdravotních hrozbách a o zrušení rozhodnutí č. 1082/2013/EU, odkaz bude aktualizován, jakmile bude návrh COM(2020) 727 final přijat].

[92]Směrnice Evropského parlamentu a Rady 2001/83/ES ze dne 6. listopadu 2001 o kodexu Společenství týkajícím se humánních léčivých přípravků (Úř. věst. L 311, 28.11.2001, s. 67).

[93] [Nařízení Evropského parlamentu a Rady o posílené úloze Evropské agentury pro léčivé přípravky při připravenosti na krize a krizovém řízení v oblasti léčivých přípravků a zdravotnických prostředků, odkaz bude aktualizován, jakmile bude návrh COM(2020) 725 final přijat].

POSTUP VE VÝBORU POŽÁDANÉM O STANOVISKO

Název	Opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a zrušení směrnice (EU) 2016/1148
Referenční údaje	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)
Příslušný výbor Datum oznámení na zasedání	ITRE 21.1.2021
Výbor, který vypracoval stanovisko Datum oznámení na zasedání	LIBE 21.1.2021
Přidružené výbory - datum oznámení na zasedání	20.5.2021
Zpravodaj(ka) Datum jmenování	Lukas Mandl 12.4.2021
Projednání ve výboru	16.6.2021 3.9.2021 11.10.2021
Datum přijetí	12.10.2021
Výsledek konečného hlasování	+: 44 –: 14 0: 4
Členové přítomní při konečném hlasování	Magdalena Adamowicz, Katarina Barley, Pernando Barrena Arza, Pietro Bartolo, Nicolas Bay, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Patrick Breyer, Saskia Bricmont, Jorge Buxadé Villalba, Damien Carême, Caterina Chinnici, Clare Daly, Marcel de Graaff, Anna Júlia Donáth, Lena Düpont, Cornelia Ernst, Laura Ferrara, Nicolaus Fest, Maria Grapini, Sophia in ‘t Veld, Patryk Jaki, Marina Kaljurand, Assita Kanko, Fabienne Keller, Peter Kofod, Moritz Körner, Jeroen Lenaers, Juan Fernando López Aguilar, Lukas Mandl, Roberta Metsola, Nadine Morano, Javier Moreno Sánchez, Maite Pagazaurtundúa, Nicola Procaccini, Emil Radev, Paulo Rangel, Terry Reintke, Diana Riba i Giner, Ralf Seekatz, Michal Šimečka, Birgit Sippel, Sara Skyttedal, Martin Sonneborn, Tineke Strik, Ramona Strugariu, Annalisa Tardino, Milan Uhrík, Tom Vandendriessche, Bettina Vollath, Elissavet Vozemberg-Vrionidi, Jadwiga Wiśniewska, Javier Zarzalejos
Náhradníci přítomní při konečném hlasování	Olivier Chastel, Tanja Fajon, Jan-Christoph Oetjen, Philippe Olivier, Anne-Sophie Pelletier, Thijs Reuten, Rob Rooken, Maria Walsh

JMENOVITÉ KONEČNÉ HLASOVÁNÍ
VE VÝBORU POŽÁDANÉM O STANOVISKO

44	+
ID	Nicolas Bay, Nicolaus Fest, Peter Kofod, Philippe Olivier, Annalisa Tardino, Tom Vandendriessche
NI	Laura Ferrara
PPE	Magdalena Adamowicz, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Lena Düpont, Jeroen Lenaers, Lukas Mandl, Roberta Metsola, Nadine Morano, Emil Radev, Paulo Rangel, Ralf Seekatz, Sara Skyttedal, Elissavet Vozemberg-Vrionidi, Maria Walsh, Javier Zarzalejos
Renew	Olivier Chastel, Anna Júlia Donáth, Sophia in 't Veld, Fabienne Keller, Moritz Körner, Jan-Christoph Oetjen, Maite Pagazaurtundúa, Michal Šimečka, Ramona Strugariu
S&D	Katarina Barley, Pietro Bartolo, Caterina Chinnici, Tanja Fajon, Maria Grapini, Marina Kaljurand, Juan Fernando López Aguilar, Javier Moreno Sánchez, Thijs Reuten, Birgit Sippel, Bettina Vollath
Verts/ALE	Damien Carême

14	-
ECR	Jorge Buxadé Villalba, Patryk Jaki, Assita Kanko, Nicola Procaccini, Rob Rooken, Jadwiga Wiśniewska
ID	Marcel de Graaff
NI	Martin Sonneborn, Milan Uhrík
Verts/ALE	Patrick Breyer, Saskia Bricmont, Terry Reintke, Diana Riba i Giner, Tineke Strik

4	0
The Left	Pernando Barrena Arza, Clare Daly, Cornelia Ernst, Anne-Sophie Pelletier

Význam zkratek:
+ : pro
- : proti
0 : zdrželi se