Úřední věstník C 328

Evropské unie

České vydání

Ročník 66

18. září 2023

Informace a oznámení

Obsah

CS

[1] Text s významem pro EHP.

([1]) Text s významem pro EHP.

II

(Sdělení)

SDĚLENÍ ORGÁNŮ, INSTITUCÍ A JINÝCH SUBJEKTŮ EVROPSKÉ UNIE

EVROPSKÁ KOMISE

Bez námitek k navrhovanému spojení

(Věc M.11106 – STELLANTIS / MICHELIN / FORVIA / SYMBIO)

(Text s významem pro EHP)

(2023/C 328/01)

Dne 17. července 2023 se Komise rozhodla nevznášet proti výše uvedenému oznámenému spojení námitky a prohlásit jej za slučitelné s vnitřním trhem. Základem tohoto rozhodnutí je ustanovení čl. 6 odst. 1 písm. b) nařízení Rady (ES) č. 139/2004 ([1]). Úplné znění rozhodnutí je k dispozici pouze v angličtině a bude zveřejněno poté, co z něj budou odstraněny případné skutečnosti, jež mají povahu obchodního tajemství. Znění tohoto rozhodnutí bude k dispozici:

— v oddílu týkajícím se spojení podniků na internetových stránkách Komise věnovaných hospodářské soutěži (https://competition-cases.ec.europa.eu/search). Tato internetová stránka umožňuje vyhledávat jednotlivá rozhodnutí o spojení podniků, a to podle společnosti, čísla případu, data a indexu hospodářského odvětví,

— v elektronické podobě na internetových stránkách EUR-Lex (http://eur-lex.europa.eu/homepage.html?locale=cs) pod číslem 32023M11106. Stránky EUR-Lex umožňují přístup k právu Evropské unie po internetu.

([1]) Úř. věst. L 24, 29.1.2004, s. 1.

SDĚLENÍ KOMISE

Pokyny Komise k uplatňování čl. 4 odst. 1 a 2 směrnice (EU) 2022/2555 (směrnice NIS 2)

(2023/C 328/02)

I. ÚVOD

1. Podle čl. 4 odst. 3 směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (směrnice NIS 2) ([1]) Komise do 17. července 2023 poskytne pokyny objasňující uplatňování čl. 4 odst. 1 a 2 uvedené směrnice.

2. Tyto pokyny objasňují uplatňování těch ustanovení, jež se týkají vztahu mezi směrnicí (EU) 2022/2555 a stávajícími a budoucími odvětvovými právními akty Unie, které se zabývají opatřeními k řízení kybernetických bezpečnostních rizik nebo požadavky na oznamování incidentů. V dodatku k těmto pokynům jsou uvedeny odvětvové právní akty Unie, které podle Komise spadají do oblasti působnosti článku 4 směrnice (EU) 2022/2555. Skutečnost, že určitý akt není v tomto dodatku uveden, nemusí nutně znamenat, že nespadá do oblasti působnosti uvedeného ustanovení.

3. Při uplatňování čl. 4 odst. 3 třetí věty směrnice (EU) 2022/2555 Komise před přijetím těchto pokynů zohlednila připomínky skupiny pro spolupráci v oblasti bezpečnosti sítí a informací a Agentury Evropské unie pro kybernetickou bezpečnost (dále jen „agentura ENISA“).

4. Těmito pokyny není dotčen výklad práva Unie Soudním dvorem Evropské unie.

II. ROVNOCENNOST POŽADAVKŮ NA KYBERNETICKOU BEZPEČNOST V ODVĚTVOVÝCH PRÁVNÍCH AKTECH UNIE

5. V čl. 4 odst. 1 směrnice (EU) 2022/2555 se stanoví, že pokud odvětvové právní akty Unie vyžadují, aby základní nebo důležité subjekty přijaly opatření k řízení kybernetických bezpečnostních rizik nebo aby oznamovaly významné incidenty, a pokud je účinek těchto opatření alespoň rovnocenný účinku povinností stanovených v uvedené směrnici, příslušná ustanovení směrnice (EU) 2022/2555, včetně ustanovení o dohledu a vymáhání stanovených v kapitole VII uvedené směrnice, se na takové subjekty nepoužijí. Toto ustanovení dále uvádí, že pokud se odvětvové právní akty Unie nevztahují na všechny subjekty v konkrétním odvětví, jež náleží do oblasti působnosti směrnice (EU) 2022/2555, použijí se nadále na subjekty, na něž se uvedené odvětvové právní akty Unie nevztahují, příslušná ustanovení uvedené směrnice.

II.1. Požadavky na řízení kybernetických bezpečnostních rizik

6. V čl. 4 odst. 2 písm. a) směrnice (EU) 2022/2555 se stanoví, že účinek opatření k řízení kybernetických bezpečnostních rizik, která jsou základní nebo důležité subjekty povinny přijmout podle odvětvových právních aktů Unie, se považuje za rovnocenný účinku povinností stanovených ve směrnici (EU) 2022/2555, pokud je účinek těchto opatření přinejmenším rovnocenný účinku opatření stanovených v čl. 21 odst. 1 a 2 uvedené směrnice. Při posuzování toho, zda je účinek požadavků na opatření k řízení kybernetických bezpečnostních rizik v odvětvovém právním aktu Unie přinejmenším rovnocenný účinku požadavků stanovených v čl. 21 odst. 1 a 2 směrnice (EU) 2022/2555, by požadavky v tomto odvětvovém právním aktu Unie měly přinejmenším odpovídat požadavkům uvedených ustanovení nebo jít nad jejich rámec, což znamená, že odvětvová ustanovení mohou být ve srovnání s odpovídajícími ustanoveními směrnice (EU) 2022/2555 věcně podrobnější.

([1]) Úř. věst. L 333, 27.12.2022, s. 80.

7. Podle čl. 21 odst. 1 prvního pododstavce směrnice (EU) 2022/2555 členské státy zajistí, aby základní a důležité subjekty přijaly vhodná a přiměřená technická, provozní a organizační opatření k řízení bezpečnostních rizik, jimž čelí sítě a informační systémy, jež tyto subjekty používají pro svůj provoz nebo poskytování svých služeb. Tato opatření by měla být založena na rizicích a měla by být schopna předcházet incidentům nebo minimalizovat jejich dopad. V čl. 21 odst. 1 druhém pododstavci směrnice (EU) 2022/2555 je uvedeno, jak by měla být posuzována přiměřenost těchto opatření ([2]). Povinnost stanovená v čl. 21 odst. 1 směrnice (EU) 2022/2555, která vyžaduje, aby základní a důležité subjekty přijaly vhodná a přiměřená opatření k řízení kybernetických bezpečnostních rizik, se vztahuje na všechny operace a služby dotčeného subjektu, nikoli pouze na konkrétní aktiva informačních technologií (dále jen „IT“) nebo kritické služby, které subjekt poskytuje.

8. Při posuzování rovnocennosti odvětvového právního aktu Unie s příslušnými ustanoveními směrnice (EU) 2022/2555 o řízení kybernetických rizik je třeba věnovat zvláštní pozornost otázce, zda povinnosti v oblasti bezpečnosti v uvedeném právním aktu zahrnují opatření zaměřená na zajištění bezpečnosti sítí a informačních systémů. Definice „bezpečnosti sítí a informačních systémů“ stanovená v čl. 6 bodě 2 směrnice (EU) 2022/2555 poukazuje na schopnost sítí a informačních systémů odolávat s určitou spolehlivostí veškerým událostem, které mohou narušit dostupnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo zpracovávaných dat nebo služeb, které jsou nabízeny prostřednictvím sítí a informačních systémů nebo které jsou jejich prostřednictvím přístupné. Použití pojmů „dostupnost“, „autenticita“, „integrita“ a „důvěrnost“ v této definici se vztahuje na všechny čtyři cíle ochrany související s bezpečností sítí a informačních systémů. Pojem „sítě a informační systémy“, jak je definován v čl. 6 bodě 1 směrnice (EU) 2022/2555, zahrnuje sítě elektronických komunikací ([3]); zařízení nebo skupinu vzájemně propojených nebo souvisejících zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování digitálních dat, a digitální data, jež jsou těmito sítěmi elektronických komunikací nebo zařízeními uchovávána, zpracovávána, opětovně vyhledávána nebo předávána za účelem jejich provozu, použití, ochrany nebo údržby. Bezpečnostní opatření vyžadovaná odvětvovým právním aktem Unie by se proto měla vztahovat také na hardware, firmware a software používaný při činnostech subjektu.

9. Dalším důležitým hlediskem při posuzování rovnocennosti odvětvového právního aktu Unie s požadavky čl. 21 odst. 1 a 2 směrnice (EU) 2022/2555 je, že opatření k řízení kybernetických bezpečnostních rizik požadovaná uvedeným aktem by měla být založena na přístupu zohledňujícím všechna rizika. Vzhledem k tomu, že hrozby pro bezpečnost sítí a informačních systémů mohou mít různý původ, může mít jakýkoli typ události negativní dopad na sítě a informační systémy subjektu a potenciálně vést k incidentu. Opatření k řízení kybernetických bezpečnostních rizik přijatá subjektem by proto měla chránit nejen sítě a informační systémy subjektu, ale také fyzické prostředí těchto systémů před jakoukoli událostí, jako je sabotáž, krádež, požár, povodeň, výpadky telekomunikací nebo elektrického proudu, nebo před neoprávněným fyzickým přístupem, jež by mohly narušit dostupnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo zpracovávaných dat nebo služeb, které tyto sítě a informační systémy nabízejí nebo které jsou jejich prostřednictvím přístupné. Opatření k řízení kybernetických bezpečnostních rizik vyžadovaná odvětvovým právním aktem Unie by se proto měla konkrétně zabývat fyzickou a environmentální bezpečností sítí a informačních systémů před selháním systému, lidskou chybou, zlovolnými činy nebo přírodními jevy ([4]).

10. Ustanovení čl. 21 odst. 2 směrnice (EU) 2022/2555 dále vyžaduje, aby opatření k řízení kybernetických bezpečnostních rizik zahrnovala konkrétní bezpečnostní požadavky uvedené v odst. 2 písm. a) až j) uvedeného ustanovení. Tyto požadavky zahrnují opatření, jako je politika analýzy rizik a bezpečnosti informačních systémů, řešení incidentů, řízení kontinuity provozu, krizové řízení, bezpečnost dodavatelského řetězce, politiky a postupy týkající se používání kryptografie a případně šifrování. Podle čl. 21 odst. 5 druhého pododstavce směrnice (EU) 2022/2555 je Komise zmocněna přijímat prováděcí akty, kterými stanoví technické, metodické a případně odvětvové požadavky, pokud jde o bezpečnostní opatření uvedená v čl. 21 odst. 2 uvedené směrnice. Pokud jde

([2]) Viz také 78., 81. a 82. bod odůvodnění směrnice (EU) 2022/2555.

([3]) Ustanovení čl. 2 odst. 1 směrnice Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví evropský kodex pro elektronické komunikace (Úř. věst. L 321, 17.12.2018, s. 36).

([4]) Viz 79. bod odůvodnění směrnice (EU) 2022/2555.

o provozovatele systému jmen domén (dále jen „provozovatelé DNS“), registry domén nejvyšší úrovně (dále jen „registry TLD“), poskytovatele služeb cloud computingu, poskytovatele služeb datových center, poskytovatele sítí pro doručování obsahu, poskytovatele řízených služeb, poskytovatele řízených bezpečnostních služeb, poskytovatele on-line tržišť, internetových vyhledávačů a služeb platforem sociálních sítí a poskytovatele služeb vytvářejících důvěru, přijme Komise do 17. října 2024 prováděcí akty týkající se technických a metodických požadavků bezpečnostní opatření uvedených v čl. 21 odst. 2 směrnice (EU) 2022/2555. Prováděcí akty dále podrobněji upřesňují hlavní podmínky a kritéria provádění stanovené v základním aktu, aniž by byla dotčena podstata uvedeného aktu ([5]).

II.2. **Požadavky na oznamování**

11. Ustanovení čl. 4 odst. 2 písm. b) směrnice (EU) 2022/2555 stanoví, že účinek požadavků na oznamování týkajících se oznamování významných incidentů se považuje za rovnocenný účinku povinností stanovených v uvedené směrnici, pokud odvětvový právní akt Unie poskytuje okamžitý, případně automatický a přímý přístup k oznámením o incidentech týmům pro reakce na počítačové bezpečnostní incidenty (dále jen „týmy CSIRT“), příslušným orgánům nebo jednotným kontaktním místům, a účinek požadavků na oznamování významných incidentů je přinejmenším rovnocenný účinku požadavků stanovených v čl. 23 odst. 1 až 6 směrnice (EU) 2022/2555.

12. Vzhledem k tomu, že účinek požadavků odvětvového právního aktu Unie na oznamování významných incidentů musí být přinejmenším rovnocenný účinku požadavků stanovených v čl. 23 odst. 1 až 6 směrnice (EU) 2022/2555, aby se tento akt mohl použít namísto oznamovacích povinností podle uvedené směrnice, jsou požadavky stanovené v čl. 23 odst. 1 až 6 směrnice pro posouzení rovnocennosti obzvláště důležité. Ustanovení čl. 23 odst. 1 až 6 směrnice (EU) 2022/2555 podrobněji stanoví, jaké druhy incidentů musí být oznamovány, komu, v jakém časovém rámci a s jakým obsahem informací. To je podrobněji vysvětleno v následujících pododdílech:

II.2.1. *Oznamování významných incidentů týmům CSIRT, příslušným orgánům a příjemcům*

13. Ustanovení čl. 23 odst. 1 prvního pododstavce první věty směrnice (EU) 2022/2555 vyžaduje, aby základní a důležité subjekty oznamovaly bez zbytečného odkladu svému týmu CSIRT nebo případně svému příslušnému orgánu každý významný incident. Podle čl. 23 odst. 1 prvního pododstavce druhé věty směrnice (EU) 2022/2555 musí základní a důležité subjekty v příslušných případech oznámit bez zbytečného odkladu příjemci svých služeb významné incidenty, které by mohly negativně ovlivnit poskytování těchto služeb.

14. Zatímco čl. 6 bod 6 směrnice (EU) 2022/2555 definuje „incidenty“ velmi široce jako jakoukoli událost narušující dostupnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo zpracovávaných dat nebo služeb, které jsou nabízeny prostřednictvím sítí a informačních systémů nebo které jsou jejich prostřednictvím přístupné, čl. 23 odst. 1 uvedené směrnice ukládá povinnost oznamovat pouze významné incidenty. Incident je významný, jestliže dotčenému subjektu způsobil nebo může způsobit závažné provozní narušení služeb nebo finanční ztráty (čl. 23 odst. 3 písm. a)) nebo způsobil nebo může způsobit jiným fyzickým nebo právnickým osobám značnou hmotnou nebo nehmotnou újmu (čl. 23 odst. 3 písm. b)).

([5]) Viz kapitola D „Další pravidla provádějící základní akt“ Nezávazných kritérií pro uplatňování článků 290 a 291 Smlouvy o fungování Evropské unie – 18. června 2019 (Úř. věst. C 223, 3.7.2019, s. 1).

15. Ve 101. bodu odůvodnění směrnice (EU) 2022/2555 se objasňuje, že oznamování incidentů by mělo vycházet z prvotního posouzení provedeného dotčeným subjektem. Při tomto prvotním posouzení by měly být mimo jiné zohledněny dotčené sítě a informační systémy, a zejména jejich význam při poskytování služeb subjektu, závažnost a technické charakteristiky kybernetické hrozby a veškeré související zranitelnosti, které jsou využívány, jakož i zkušenosti subjektu s podobnými incidenty. Ukazatele, jako jsou rozsah, v jakém je ovlivněno fungování služby, doba trvání incidentu nebo počet dotčených příjemců služeb, by mohly hrát důležitou úlohu při určování toho, zda je provozní narušení služby závažné.

16. Podle čl. 23 odst. 11 druhého pododstavce směrnice (EU) 2022/2555 je Komise zmocněna přijímat prováděcí akty dále upřesňující případy, kdy se incident považuje za významný. Pokud jde o provozovatele DNS, registry domén nejvyšší úrovně, poskytovatele služeb cloud computingu, poskytovatele služeb datových center, poskytovatele sítí pro doručování obsahu, poskytovatele řízených služeb, poskytovatele řízených bezpečnostních služeb, poskytovatele on-line tržišť, internetových vyhledávačů a služeb platforem sociálních sítí, přijme Komise tyto prováděcí akty do 17. října 2024. Prováděcí akty dále podrobněji upřesňují hlavní podmínky a kritéria provádění stanovené v základním aktu, aniž by byla dotčena podstata uvedeného aktu ([6]).

II.2.2. *Vícefázový přístup a časový rámec týkající se oznamování významných incidentů*

17. Směrnice (EU) 2022/2555 stanoví vícefázový přístup k oznamování významných incidentů, který zahrnuje včasné varování, oznámení incidentu a závěrečnou zprávu. Tyto tři prvky mohou být případně doplněny průběžnými zprávami a zprávou o pokroku.

18. Cílem vícefázového přístupu je dosáhnout správné rovnováhy mezi rychlým oznamováním, které pomáhá snížit potenciální šíření významných incidentů a umožňuje základním a důležitým subjektům žádat o podporu, na jedné straně a podrobným oznamováním, které čerpá cenná poučení z jednotlivých incidentů a s postupem času zvyšuje kybernetickou odolnost jednotlivých subjektů a celých odvětví, na straně druhé ([7]).

19. Podle vícefázového přístupu musí zásadní a důležité subjekty nejprve bez zbytečného odkladu, nejpozději však do 24 hodin po zjištění významného incidentu, předložit příslušnému týmu CSIRT nebo orgánu včasné varování. Následně musí tyto subjekty bez zbytečného odkladu, nejpozději však do 72 hodin po zjištění významného incidentu, předložit oznámení incidentu. Poté si může příslušný tým CSIRT nebo orgán vyžádat průběžnou zprávu. Závěrečná zpráva musí být příslušnému týmu CSIRT nebo orgánu předložena nejpozději do jednoho měsíce od předložení oznámení incidentu, ledaže incident v té době stále trvá; v takovém případě musí být předložena zpráva o pokroku a následně, do jednoho měsíce po vyřešení incidentu, závěrečná zpráva.

20. Na oznámení incidentu stanovené v čl. 23 odst. 4 druhém pododstavci směrnice (EU) 2022/2555 se ve vztahu k poskytovatelům služeb vytvářejících důvěru vztahuje jiný časový rámec. Tito poskytovatelé musí oznamovat významné incidenty týkající se jimi poskytovaných služeb vytvářejících důvěru bez zbytečného odkladu, nejpozději však do 24 hodin od okamžiku, kdy se o významném incidentu dozvěděli.

([6]) Viz kapitola D „Další pravidla provádějící základní akt“ Nezávazných kritérií pro uplatňování článků 290 a 291 Smlouvy o fungování Evropské unie – 18. června 2019 (Úř. věst. C 223, 3.7.2019, s. 1).

([7]) Viz 101. bod odůvodnění směrnice (EU) 2022/2555.

II.2.3. *Obsah povinnosti oznamovat významné incidenty týmům CSIRT nebo příslušným orgánům*

21. Jako obecné pravidlo platí, že podle čl. 23 odst. 1 prvního pododstavce třetí věty směrnice (EU) 2022/2555 musí členské státy zajistit, aby základní a důležité subjekty oznamovaly mimo jiné všechny informace, které týmu CSIRT nebo případně příslušnému orgánu umožní posoudit případný přeshraniční dopad daného incidentu. Tento požadavek týkající se obsahu oznamovací povinnosti je dále upřesněn v čl. 23 odst. 4 směrnice (EU) 2022/2555, který stanoví vícefázový přístup.

22. Podle čl. 23 odst. 4 písm. a) musí včasné varování případně obsahovat údaj o tom, zda existuje podezření, že významný incident byl způsoben nezákonným nebo svévolným zásahem nebo že by mohl mít (zda je pravděpodobné, že bude mít) přeshraniční dopad. Podle 102. bodu odůvodnění směrnice (EU) 2022/2555 by včasné varování mělo zahrnovat pouze informace nezbytné k tomu, aby se příslušný tým CSIRT nebo orgán dozvěděly o významném incidentu a aby dotčený subjekt mohl v případě potřeby požádat o pomoc.

23. Oznámení incidentu musí případně obsahovat aktualizace informací předložených v rámci včasného varování. Kromě toho musí zahrnovat prvotní posouzení významného incidentu, včetně jeho závažnosti a dopadu, a pokud jsou k dispozici, také indikátory narušení.

24. V případě, že je požadována průběžná zpráva, musí obsahovat podstatné aktualizace stavu. Závěrečná zpráva musí zahrnovat podrobný popis incidentu včetně jeho závažnosti a dopadu, druh hrozby nebo základní příčinu, která incident pravděpodobně spustila, učiněná a probíhající opatření ke zmírnění následků a případně přeshraniční dopad incidentu.

II.2.4. *Okamžitý přístup k oznámením o incidentech*

25. V čl. 4 odst. 2 písm. b) směrnice (EU) 2022/2555 se stanoví, že aby byl odvětvový právní akt Unie použitelný s ohledem na požadavky na oznamování namísto uvedené směrnice, musí poskytnout týmům CSIRT, příslušným orgánům nebo jednotným kontaktním místům podle směrnice (EU) 2022/2555 okamžitý přístup k oznámením o incidentech předloženým v souladu s odvětvovým právním aktem Unie. V souladu s 24. bodem odůvodnění směrnice (EU) 2022/2555 lze takový okamžitý přístup zajistit tak, že oznámení o incidentech budou týmu CSIRT, příslušnému orgánu nebo jednotnému kontaktnímu místu předávána bez zbytečného odkladu.

26. Okamžitý přístup lze zajistit prostřednictvím automatických a přímých prostředků, které by členské státy měly případně zavést. Mechanismy automatického a přímého oznamování zajišťují při vyřizování oznámení o incidentech systematické a okamžité sdílení informací s týmy CSIRT, příslušnými orgány nebo jednotnými kontaktními místy. Pro zjednodušení oznamování a zavedení mechanismu automatického a přímého oznamování by členské státy mohly rovněž využít jednotné kontaktní místo, které musí být v souladu s odvětvovým právním aktem Unie.

27. Při posuzování toho, zda je účinek požadavků na oznamování významných incidentů v odvětvovém právním aktu Unie přinejmenším rovnocenný účinku požadavků stanovených v čl. 23 odst. 1 až 6 směrnice (EU) 2022/2555, by požadavky v uvedeném odvětvovém právním aktu Unie měly přinejmenším odpovídat požadavkům čl. 23 odst. 1 až 6 nebo by měly být podrobnější než uvedená ustanovení. Požadavky by se měly vztahovat na druh incidentů, které je třeba oznamovat podle směrnice (EU) 2022/2555, zejména s ohledem na příjemce, obsah a příslušné časové rámce.

III. **DŮSLEDKY ROVNOCENNOSTI**

III.1. **Dohled a vymáhání**

28. Pokud je účinek odvětvových právních aktů Unie přinejmenším rovnocenný účinku povinností stanovených ve směrnici (EU) 2022/2555, nejenže se nepoužijí příslušná ustanovení uvedené směrnice týkající se povinnosti přijmout opatření k řízení kybernetických bezpečnostních rizik nebo oznamovat významné incidenty, ale ani ustanovení o dohledu a vymáhání stanovená v kapitole VII směrnice (EU) 2022/2555.

29. V 25. bodu odůvodnění směrnice (EU) 2022/2555 se vysvětluje, že odvětvové právní akty Unie, které mají přinejmenším rovnocenný účinek, by mohly stanovit, že příslušné orgány podle těchto aktů vykonávají své pravomoci v oblasti dohledu a vymáhání v souvislosti s řízením kybernetických bezpečnostních rizik nebo oznamovacími povinnostmi za pomoci příslušných orgánů podle směrnice (EU) 2022/2555. Dotčené příslušné orgány by za tímto účelem mohly uzavřít ujednání o spolupráci, včetně postupů týkajících se koordinace činností v oblasti dohledu, postupů pro vyšetřování a kontrol na místě v souladu s vnitrostátními právními předpisy a mechanismu pro výměnu příslušných informací o dohledu a vymáhání mezi příslušnými orgány. Tento mechanismus pro výměnu příslušných informací by mohl zahrnovat přístup ke kybernetickým údajům, které si vyžádají příslušné orgány podle směrnice (EU) 2022/2555.

III.2. **Národní strategie kybernetické bezpečnosti**

30. Každý členský stát je podle čl. 7 odst. 1 směrnice (EU) 2022/2555 povinen přijmout národní strategii kybernetické bezpečnosti. Národní strategie kybernetické bezpečnosti je soudržný rámec členského státu vymezující strategické cíle a priority v oblasti kybernetické bezpečnosti a správy za účelem jejich dosažení v tomto členském státě (viz čl. 6 bod 4 směrnice (EU) 2022/2555). Strategie kybernetické bezpečnosti musí mimo jiné zahrnovat cíle a priority zahrnující zejména odvětví uvedená v přílohách I a II směrnice (EU) 2022/2555. Kromě toho musí tato strategie zahrnovat rámec správy k dosažení těchto cílů a priorit, včetně politik uvedených v čl. 7 odst. 2 směrnice (EU) 2022/2555.

31. Kromě toho čl. 7 odst. 1 písm. c) směrnice (EU) 2022/2555 stanoví, že vnitrostátní strategie kybernetické bezpečnosti musí zahrnovat rámec správy, který vyjasňuje úlohy a povinnosti příslušných zúčastněných stran na vnitrostátní úrovni, na němž se zakládá spolupráce a koordinace na vnitrostátní úrovni mezi příslušnými orgány, jednotnými kontaktními místy a týmy CSIRT podle směrnice (EU) 2022/2555, jakož i koordinace a spolupráce mezi těmito subjekty a příslušnými orgány podle odvětvových právních aktů Unie.

32. Požadavek na přijetí strategie kybernetické bezpečnosti podle článku 7 směrnice (EU) 2022/2555 se tedy netýká ani požadavků na kybernetickou bezpečnost uložených základním a důležitým subjektům podle článků 21 a 23 uvedené směrnice, ani ustanovení týkajících se dohledu nad nimi a jejich vymáhání stanovených v kapitole VII, jak požaduje čl. 4 odst. 1 a 2 uvedené směrnice. Příslušné ustanovení článku 7 by se mělo nadále používat s ohledem na odvětví, pododvětví a typy subjektů, pro které existují odvětvové právní akty Unie ve smyslu článku 4 směrnice (EU) 2022/2555.

III.3. **Určení týmu CSIRT**

33. Podle čl. 10 odst. 1 směrnice (EU) 2022/2555 musí členské státy určit nebo zřídit jeden nebo více týmů CSIRT, které pokrývají alespoň odvětví, pododvětví a druhy subjektů uvedené v přílohách I a II směrnice, tedy včetně odvětví, pododvětví a druhů subjektů, pro které existují odvětvové právní akty Unie. Týmy CSIRT budou v tomto ohledu obvykle plnit také úkoly stanovené v čl. 11 odst. 3 směrnice (EU) 2022/2555, pokud nejsou v odvětvových právních aktech Unie stanoveny konkrétní úkoly.

III.4. **Národní rámce řešení kybernetických krizí a síť EU-CyCLONe**

34. Podle čl. 9 odst. 1 směrnice (EU) 2022/2555 musí členské státy určit nebo zřídit jeden nebo více orgánů pro řešení kybernetických krizí, které jsou odpovědné za řízení rozsáhlých kybernetických bezpečnostních incidentů a krizí. Podle čl. 6 bodu 7 uvedené směrnice se rozsáhlým kybernetickým bezpečnostním incidentem rozumí incident, který způsobí úroveň narušení, jež přesahuje schopnost členského státu na takový incident reagovat, nebo který má významný dopad na nejméně dva členské státy. Ustanovení čl. 9 odst. 4 směrnice (EU) 2022/2555 vyžaduje, aby členské státy rovněž přijaly národní plán reakce na rozsáhlé kybernetické bezpečnostní incidenty a krize, v němž budou stanoveny cíle a ujednání řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí. Tento plán by měl mimo jiné stanovit postupy pro řešení kybernetických krizí, včetně jejich začlenění do obecného vnitrostátního rámce pro krizové řízení, a kanály pro výměnu informací, a příslušné veřejné a soukromé zúčastněné strany a zapojenou infrastrukturu. Tyto postupy pro řešení kybernetických krizí a příslušné veřejné a soukromé zúčastněné strany a infrastruktura mohou zahrnovat postupy a zúčastněné strany specifické pro dané odvětví.

35. Článkem 16 směrnice (EU) 2022/2555 se zřizuje Evropská síť styčných organizací pro řešení kybernetických krizí (EU-CyCLONe), jejímž účelem je podporovat koordinované řízení rozsáhlých kybernetických bezpečnostních incidentů a krizí na operativní úrovni a zajišťovat pravidelné výměny relevantních informací mezi členskými státy a orgány, institucemi a jinými subjekty Unie.

36. Vzhledem k tomu, že článek 9 o rámcích řešení kybernetických krizí a článek 16 o síti EU-CyCLONe se netýkají požadavků na kybernetickou bezpečnost uložených subjektům podle článků 21 a 23 směrnice (EU) 2022/2555 ani dohledu a vymáhání stanovených v kapitole VII, jak vyžaduje čl. 4 odst. 1 a 2 uvedené směrnice, měly by se články 9 a 16 použít pro odvětví v plném rozsahu, a to i přes existenci odvětvových právních aktů Unie ve smyslu článku 4. V důsledku toho musí členské státy určit nebo zřídit jeden nebo více orgánů pro řešení kybernetických krizí odpovědných za řízení rozsáhlých kybernetických bezpečnostních incidentů a krizí, k nimž dochází v odvětvích, na něž se vztahují odvětvové právní akty Unie. Při přijímání národního plánu reakce na rozsáhlé kybernetické bezpečnostní incidenty a krize by navíc neměla být opomenuta odvětví, na která se vztahují odvětvové právní akty Unie. V neposlední řadě by síť EU-CyCLONe měla plnit své úkoly zakotvené v článku 16 směrnice (EU) 2022/2555, pokud jde o odvětví, v nichž se na subjekty vztahují odvětvové právní akty Unie.

III.5. **Vyloučení použití čl. 3 odst. 3 a 4, článku 20 a čl. 27 odst. 2 a 3**

37. Podle čl. 3 odst. 3 směrnice (EU) 2022/2555 jsou členské státy povinny vytvořit seznam základních a důležitých subjektů, jakož i subjektů poskytujících služby registrace jmen domén, které spadají do oblasti působnosti směrnice. Podle čl. 27 odst. 2 členské státy vyžadují, aby subjekty uvedené v čl. 27 odst. 1 uvedené směrnice předložily příslušným orgánům určité informace. Vzhledem k tomu, že účelem těchto ustanovení je zajistit jasný přehled o subjektech spadajících do oblasti působnosti směrnice (EU) 2022/2555 s cílem podpořit dohled nad základními a důležitými subjekty spadajícími do její působnosti, vyplývá z toho, že by se tato ustanovení neměla vztahovat na subjekty, pro které platí odvětvový právní akt Unie, pokud jde o požadavky na řízení kybernetických bezpečnostních rizik a oznamování. To nebrání členským státům, aby tyto subjekty na seznam zařadily.

Podle čl. 20 odst. 1 směrnice (EU) 2022/2555 jsou řídicí orgány základních a důležitých subjektů povinny schvalovat opatření k řízení kybernetických bezpečnostních rizik přijatá těmito subjekty za účelem dosažení souladu s článkem 21, dohlížet nad jeho uplatňováním a mohou nést odpovědnost, poruší-li subjekty uvedený článek. Podle čl. 20 odst. 2 uvedené směrnice členské státy zajistí, aby členové řídících orgánů základních a důležitých subjektů museli absolvovat školení, a vybízí základní a důležité subjekty, aby pravidelně nabízely podobné školení svým zaměstnancům, aby tak získali dostatečné znalosti a dovednosti, aby mohli identifikovat rizika a posoudit postupy řízení kybernetických bezpečnostních rizik a jejich dopad na služby poskytované subjektem. Vzhledem k tomu, že povinnosti vyplývající z článku 20 směrnice (EU) 2022/2555 jsou neoddělitelně spjaty s požadavky článku 21 uvedené směrnice, vyplývá z toho, že by se článek 20 neměl použít v případě odvětvových právních aktů Unie ve smyslu článku 4 uvedené směrnice, které se vztahují na požadavky na řízení kybernetických bezpečnostních rizik.

DODATEK

Odvětvové právní akty Unie

Nařízení (EU) 2022/2554 (akt o digitální provozní odolnosti) ([1])

1. Ustanovení čl. 1 odst. 2 nařízení (EU) 2022/2554 (akt o digitální provozní odolnosti) stanoví, že ve vztahu k finančním subjektům, na něž se vztahuje směrnice (EU) 2022/2555 a odpovídající vnitrostátní prováděcí pravidla, se nařízení (EU) 2022/2554 pro účely článku 4 směrnice (EU) 2022/2555 považuje za odvětvový právní akt Unie. Toto ustanovení se odráží v 28. bodě odůvodnění směrnice (EU) 2022/2555, v němž se uvádí, že akt o digitální provozní odolnosti by měl být považován za odvětvový právní akt Unie ve vztahu ke směrnici (EU) 2022/2555, pokud jde o finanční subjekty. V důsledku toho se namísto ustanovení směrnice (EU) 2022/2555 použijí ustanovení nařízení (EU) 2022/2554 týkající se řízení rizik v oblasti informačních a komunikačních technologií (dále jen „IKT“) (článek 6 a následující), řízení incidentů souvisejících s IKT, a zejména oznamování závažných incidentů souvisejících s IKT (článek 17 a následující), jakož i testování digitální provozní odolnosti, (článek 24 a následující), ujednání o sdílení informací (článek 25) a rizika v oblasti IKT spojeného s třetími stranami (článek 28 a následující). Členské státy by proto neměly na finanční subjekty, na které se vztahuje nařízení (EU) 2022/2554, uplatňovat ustanovení směrnice (EU) 2022/2555 o povinnostech týkajících se řízení kybernetických bezpečnostních rizik a oznamování a o dohledu a vymáhání.

2. V tomto ohledu jsou finanční subjekty považovány za subjekty uvedené v čl. 2 odst. 1 písm. a) až t) nařízení (EU) 2022/2554. Mezi druhy subjektů, které spadají do oblasti působnosti nařízení (EU) 2022/2554 jako finanční subjekty, jakož i do oblasti působnosti směrnice (EU) 2022/2555 jako základní nebo důležité subjekty, patří úvěrové instituce, obchodní systémy a ústřední protistrany. Vzhledem k tomu, že je důležité udržovat pevné vztahy a výměnu informací s finančním sektorem podle směrnice (EU) 2022/2555, mohou evropské orgány dohledu a příslušné orgány podle nařízení (EU) 2022/2554 požádat o účast na činnostech skupiny pro spolupráci ([2]), vyměňovat si informace a spolupracovat s jednotnými kontaktními místy, jakož i s týmy CSIRT a příslušnými orgány podle směrnice (EU) 2022/2555 ([3]). Příslušné orgány podle nařízení (EU) 2022/2554 by měly rovněž předávat podrobnosti o závažných incidentech souvisejících s IKT a případně o významných kybernetických hrozbách týmům CSIRT, příslušným orgánům nebo jednotným kontaktním místům podle směrnice (EU) 2022/2555. Toho lze dosáhnout poskytnutím okamžitého přístupu k oznámením o incidentech a jejich předáváním buď přímo, nebo prostřednictvím jednotného kontaktního místa. Týmy CSIRT by měly do svých činností zahrnout finanční odvětví ([4]). Členské státy by měly i nadále zahrnovat finanční sektor do svých strategií kybernetické bezpečnosti. Ustanovení o národních rámcích řešení kybernetických krizí (článek 9 směrnice (EU) 2022/2555), jakož i o síti EU-CyCLONe (článek 16 směrnice (EU) 2022/2555) by se měla nadále vztahovat na subjekty spadající do oblasti působnosti nařízení (EU) 2022/2554.

([1]) Nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011 (Úř. věst. L 333, 27.12.2022, s. 1).

([2]) Ustanovení čl. 14 odst. 3 směrnice (EU) 2022/2555 a čl. 47 odst. 1 nařízení (EU) 2022/2554.

([3]) Viz 28. bod odůvodnění směrnice (EU) 2022/2555.

([4]) Tamtéž.

IV

(Informace)

INFORMACE ORGÁNŮ, INSTITUCÍ A JINÝCH SUBJEKTŮ EVROPSKÉ UNIE

RADA

Oznámení určené osobám a subjektům, na něž se vztahují opatření stanovená rozhodnutím Rady 2011/235/SZBP, prováděným prováděcím rozhodnutím Rady (SZBP) 2023/1780, a nařízením Rady (EU) č. 359/2011, prováděným prováděcím nařízením Rady (EU) 2023/1779, o omezujících opatřeních namířených proti některým osobám, subjektům a orgánům s ohledem na situaci v Íránu

(2023/C 328/03)

Osobám a subjektům, které jsou uvedeny v příloze rozhodnutí Rady 2011/235/SZBP ([1]), prováděného prováděcím rozhodnutím Rady (SZBP) 2023/1780 ([2]), a v příloze I nařízení Rady (EU) č. 359/2011 ([3]), prováděného prováděcím nařízením Rady (EU) 2023/1779 ([4]), o omezujících opatřeních namířených proti některým osobám, subjektům a orgánům s ohledem na situaci v Íránu, se dávají na vědomí následující informace.

Rada Evropské unie rozhodla, že uvedené osoby a subjekty by měly být zařazeny na seznam osob a subjektů, na něž se vztahují omezující opatření stanovená rozhodnutím 2011/235/SZBP a nařízením (EU) č. 359/2011.

Dotčené osoby a subjekty se upozorňují, že mohou požádat příslušné orgány daného členského státu (členských států) uvedené na internetových stránkách, jejichž seznam je obsažen v příloze II nařízení (EU) č. 359/2011, o povolení použít zmrazené finanční prostředky na základní potřeby nebo konkrétní platby (viz článek 4 uvedeného nařízení).

Dotčené osoby a subjekty mohou před 1. lednem 2024 zaslat Radě žádost včetně podpůrných dokumentů, aby rozhodnutí o jejich zařazení na výše uvedený seznam bylo znovu zváženo, a to na tuto adresu:

Council of the European Union
General Secretariat
RELEX.1
Rue de la Loi/Wetstraat 175
1048 Bruxelles/Brussel
BELGIQUE/BELGIË

E-mail: sanctions@consilium.europa.eu

([1]) Úř. věst. L 100, 14.4.2011, s. 51.
([2]) Úř. věst. L 228 I, 15.9.2023, s. 6.
([3]) Úř. věst. L 100, 14.4.2011, s. 1.
([4]) Úř. věst. L 228 I, 15.9.2023, s. 1.

Dotčené osoby a subjekty se rovněž upozorňují, že mají možnost napadnout rozhodnutí Rady u Tribunálu Evropské unie v souladu s podmínkami stanovenými v čl. 275 druhém pododstavci a čl. 263 čtvrtém a šestém pododstavci Smlouvy o fungování Evropské unie.

Oznámení určené subjektům údajů, na něž se vztahují omezující opatření stanovená rozhodnutím Rady 2011/235/SZBP a nařízením Rady (EU) č. 359/2011 o omezujících opatřeních namířených proti některým osobám, subjektům a orgánům s ohledem na situaci v Íránu

(2023/C 328/04)

Subjektům údajů se v souladu s článkem 16 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ([1]) dávají na vědomí následující informace.

Právním základem tohoto zpracování údajů jsou rozhodnutí 2011/235/SZBP ([2]), prováděné prováděcím rozhodnutím Rady (SZBP) 2023/1780 ([3]), a nařízení (EU) č. 359/2011 ([4]), prováděné prováděcím nařízením Rady (EU) 2023/1779 ([5]).

Správcem tohoto zpracování údajů je Rada Evropské unie zastupovaná generální ředitelkou generálního ředitelství pro vnější vztahy (RELEX) generálního sekretariátu Rady a zpracováním je pověřeno oddělení RELEX.1, které lze kontaktovat na této adrese:

Council of the European Union
General Secretariat
RELEX.1
Rue de la Loi/Wetstraat 175
1048 Bruxelles/Brussel
BELGIQUE/BELGIË

E-mail: sanctions@consilium.europa.eu

Pověřence Rady pro ochranu osobních údajů lze kontaktovat na této adrese:

Data Protection Officer

data.protection@consilium.europa.eu

Účelem zpracování údajů je sestavit a aktualizovat seznam osob, na něž se vztahují omezující opatření stanovená rozhodnutím 2011/235/SZBP, prováděným prováděcím rozhodnutím (SZBP) 2023/1780, a nařízením (EU) č. 359/2011, prováděným prováděcím nařízením (EU) 2023/1779.

Subjekty údajů jsou fyzické osoby, které splňují kritéria pro zařazení na seznam stanovená rozhodnutím 2011/235/SZBP a nařízením (EU) č. 359/2011.

Mezi shromažďované osobní údaje patří údaje nezbytné ke správné identifikaci dotčené osoby, odůvodnění a veškeré další údaje související s důvody zařazení na seznam.

Právním základem pro nakládání s osobními údaji jsou rozhodnutí Rady přijatá podle článku 29 SEU a nařízení Rady přijatá podle článku 215 SFEU, která určují fyzické osoby (subjekty údajů) a ukládají zmrazení majetku a cestovní omezení.

Zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu v souladu s čl. 5 odst. 1 písm. a) a pro splnění právních povinností stanovených ve výše uvedených právních aktech, které se na správce vztahují v souladu s čl. 5 odst. 1 písm. b) nařízení (EU) 2018/1725.

Zpracování je nezbytné z důvodů významného veřejného zájmu v souladu s čl. 10 odst. 2 písm. g) nařízení (EU) 2018/1725.

Rada může získat osobní údaje subjektů údajů od členských států nebo od Evropské služby pro vnější činnost. Příjemci osobních údajů jsou členské státy, Evropská komise a Evropská služba pro vnější činnost.

([1]) Úř. věst. L 295, 21.11.2018, s. 39.
([2]) Úř. věst. L 100, 14.4.2011, s. 51.
([3]) Úř. věst. L 228 I, 15.9.2023, s. 6.
([4]) Úř. věst. L 100, 14.4.2011, s. 1.
([5]) Úř. věst. L 228 I, 15.9.2023, s. 1.

Veškeré osobní údaje zpracovávané Radou v souvislosti s autonomními omezujícími opatřeními EU budou uchovávány po dobu pěti let od okamžiku, kdy byl subjekt údajů odstraněn ze seznamu osob, na něž se vztahuje zmrazení majetku, nebo od uplynutí doby platnosti opatření nebo, bude-li podána žaloba k Soudnímu dvoru, až do vynesení pravomocného rozsudku. Osobní údaje obsažené v dokumentech zaregistrovaných Radou uchovává Rada pro účely archivace ve veřejném zájmu ve smyslu čl. 4 odst. 1 písm. e) nařízení (EU) 2018/1725.

Rada může být nucena vyměňovat si osobní údaje týkající se subjektu údajů se třetí zemí nebo mezinárodní organizací v souvislosti s prováděním označení ze strany OSN Radou nebo v rámci mezinárodní spolupráce týkající se politiky omezujících opatření EU.

Neexistuje-li rozhodnutí o odpovídající ochraně nebo vhodné záruky, vychází předání osobních údajů do třetí země nebo mezinárodní organizaci z těchto podmínek podle článku 50 nařízení (EU) 2018/1725: předání je nezbytné z důležitých důvodů veřejného zájmu; předání je nezbytné pro určení, výkon nebo obhajobu právních nároků.

Do zpracování osobních údajů subjektu údajů není zapojeno žádné automatizované rozhodování.

Subjekty údajů mají právo na informace a na přístup ke svým osobním údajům. Mají rovněž právo na opravu a doplnění svých údajů. Za určitých okolností mohou mít právo na výmaz svých osobních údajů nebo právo vznést námitku proti zpracování svých osobních údajů nebo požádat o omezení tohoto zpracování.

Subjekty údajů mohou tato práva uplatnit zasláním e-mailu správci s kopií pro pověřence pro ochranu osobních údajů, jak je uvedeno výše.

Pro potvrzení své totožnosti musí subjekty údajů ke své žádosti přiložit kopii dokladu totožnosti (průkaz totožnosti nebo cestovní pas). V tomto dokladu by mělo být uvedeno identifikační (rodné) číslo, země vydání, platnost dokladu, jméno, adresa a datum narození. Jakékoli jiné údaje obsažené v kopii tohoto dokladu totožnosti, jako jsou fotografie nebo jakékoli osobní charakteristiky, je možné začernit.

Subjekty údajů mají právo podat stížnost u evropského inspektora ochrany údajů v souladu s nařízením (EU) 2018/1725 (edps@edps.europa.eu).

Než tak učiní, doporučuje se, aby se subjekty údajů nejprve pokusily dosáhnout nápravy tím, že se obrátí na správce nebo pověřence Rady pro ochranu osobních údajů.

EVROPSKÁ KOMISE

Souhrn rozhodnutí Evropské komise týkajících se povolení k uvedení na trh za účelem použití a/nebo k použití látek uvedených v příloze XIV nařízení Evropského parlamentu a Rady (ES) č. 1907/2006 o registraci, hodnocení, povolování a omezování chemických látek

(Zveřejněno podle čl. 64 odst. 9 nařízení (ES) č. 1907/2006 ([1]))

(Text s významem pro EHP)

(2023/C 328/05)

Rozhodnutí o odnětí povolení

Odkaz na rozhodnutí ([1])	Datum rozhodnutí	Název látky	Adresát rozhodnutí	Použití, jehož se odnětí povolení týká	Zrušené rozhodnutí	Odůvodnění rozhodnutí
C(2023) 6014	11. září 2023	Dichroman sodný Číslo ES: 234-190-3; č. CAS 10588-01-9 (bezvodý) č. CAS 7789-12-0 (dihydrát)	Gruppo Colle S.r.l., Via G. Di Vittorio 3/5, 59025 Usella, Cantagallo, Prato, Itálie	Jako mořidlo při barvení vlny tmavými barvami	C(2017) 8331	Zpráva o přezkoumání neprokázala, že žadatel nemá k dispozici vhodné alternativy, v souladu s čl. 60 odst. 4 nařízení (ES) č. 1907/2006.

([1]) Rozhodnutí je dostupné na internetových stránkách Evropské komise na adrese: Povolení (europa.eu).

([1]) Úř. věst. L 396, 30.12.2006 , s. 1.

Směnné kurzy vůči euru [1]

15. září 2023

(2023/C 328/06)

1 euro =

	měna	směnný kurz		měna	směnný kurz
USD	americký dolar	1,0658	CAD	kanadský dolar	1,4409
JPY	japonský jen	157,50	HKD	hongkongský dolar	8,3416
DKK	dánská koruna	7,4573	NZD	novozélandský dolar	1,8008
GBP	britská libra	0,85878	SGD	singapurský dolar	1,4524
SEK	švédská koruna	11,8730	KRW	jihokorejský won	1 415,78
CHF	švýcarský frank	0,9554	ZAR	jihoafrický rand	20,2968
ISK	islandská koruna	145,30	CNY	čínský juan	7,7561
NOK	norská koruna	11,4220	IDR	indonéská rupie	16 379,21
BGN	bulharský lev	1,9558	MYR	malajsijský ringgit	4,9922
CZK	česká koruna	24,496	PHP	filipínské peso	60,612
HUF	maďarský forint	383,75	RUB	ruský rubl	
PLN	polský zlotý	4,6308	THB	thajský baht	38,145
RON	rumunský lei	4,9698	BRL	brazilský real	5,1860
TRY	turecká lira	28,7513	MXN	mexické peso	18,2275
AUD	australský dolar	1,6498	INR	indická rupie	88,6150

[1] *Zdroj*: referenční směnné kurzy jsou publikovány ECB.

V

(Oznámení)

ŘÍZENÍ TÝKAJÍCÍ SE PROVÁDĚNÍ POLITIKY HOSPODÁŘSKÉ SOUTĚŽE

EVROPSKÁ KOMISE

Předběžné oznámení o spojení podniků

(Věc M.11239 – EDF / CREDIT MUTUEL / ILE-DE-FRANCE BUILDING)

Věc, která může být posouzena zjednodušeným postupem

(Text s významem pro EHP)

(2023/C 328/07)

1. Komise dne 8. září 2023 obdržela oznámení o navrhovaném spojení podle článku 4 nařízení Rady (ES) č. 139/2004 ([1]).

Toto oznámení se týká těchto podniků:

— SAS C91 (Francie), kontrolovaného podnikem Électricité de France („EDF“, Francie),

— La Française Real Estate Managers („La Française“, Francie), kontrolovaného podnikem Caisse Régionale Crédit Mutuel Nord Europe (Francie), která je sama členem skupiny Crédit Mutuel (Francie),

— budovy nacházející se v regionu Ile-de-France („budova“, Francie).

Podniky EDF a Crédit Mutuel získají ve smyslu čl. 3 odst. 1 písm. b) nařízení o spojování společnou kontrolu nad celou zmiňovanou budovou.

Spojení se uskutečňuje nákupem majetku.

2. Předmětem podnikání příslušných podniků je:

— EDF: působí ve Francii a v zahraničí v oblasti výroby a velkoobchodního prodeje elektrické energie, přenosu, distribuce a dodávek elektrické energie, poskytování dalších služeb souvisejících s elektrickou energií a v menší míře v oblasti výroby a velkoobchodního a maloobchodního prodeje plynu,

— Crédit Mutuel: působí v oblasti poskytování bankovních a finančních služeb, zejména ve Francii. Skupina Crédit Mutuel nabízí prostřednictvím své dceřiné společnosti La Française služby správy nemovitostí.

3. Uvedená budova, která se nachází na adrese 111, avenue de France, 75013 Paříž (Francie), je určena pro umístění kanceláří a prodejen.

4. Komise po předběžném posouzení zjistila, že by oznamovaná transakce mohla spadat do působnosti nařízení o spojování. Konečné rozhodnutí v tomto ohledu však zůstává vyhrazeno.

([1]) Úř. věst. L 24, 29.1.2004, s. 1 („nařízení o spojování“).

V souladu se sdělením Komise o zjednodušeném postupu ohledně některých spojování podle nařízení Rady (ES) č. 139/2004 ([2]) je třeba uvést, že tato věc může být posouzena podle postupu stanoveného sdělením.

5. Komise vyzývá zúčastněné třetí strany, aby jí k navrhované transakci předložily své případné připomínky.

Připomínky musí být Komisi doručeny nejpozději do deseti dnů po zveřejnění tohoto oznámení. Je třeba vždy uvést toto číslo jednací:

M.11239 – EDF / CREDIT MUTUEL / ILE-DE-FRANCE BUILDING

Připomínky lze Komisi zaslat e-mailem nebo poštou. Použijte tyto kontaktní informace:

E-mail: COMP-MERGER-REGISTRY@ec.europa.eu

Poštovní adresa:

Commission européenne/Europese Commissie
Direction générale de la concurrence
Greffe des concentrations
1049 Bruxelles/Brussel,
BELGIQUE/BELGIË

([2]) Úř. věst. C 366, 14.12.2013, s. 5.

ISSN 1977-0863 (elektronické vydání)
ISSN 1725-5163 (papírové vydání)

Úřad pro publikace
Evropské unie
L-2985 Lucemburk
LUCEMBURSKO

CS