

Službeni list

Europske unije

C 328



Hrvatsko izdanje

Informacije i objave

Godište 66.

18. rujna 2023.

Sadržaj

II. Informacije

INFORMACIJE INSTITUCIJA, TIJELA, UREDA I AGENCIJA EUROPSKE UNIJE

Europska komisija

2023/C 328/01	Neprotivljenje prijavljenoj koncentraciji (Predmet M.11106 – STELLANTIS / MICHELIN / FORVIA / SYMBIO) ⁽¹⁾	1
2023/C 328/02	Komunikacija Komisije – Smjernice Komisije za primjenu članka 4. stavaka 1. i 2. Direktive (EU) 2022/2555 (Direktiva NIS 2)	2

IV. Obavijesti

OBAVIJESTI INSTITUCIJA, TIJELA, UREDA I AGENCIJA EUROPSKE UNIJE

Vijeće Europske unije

2023/C 328/03	Obavijest osobama i subjektima na koje se primjenjuju mjere predviđene u Odluci Vijeća 2011/235/ZVSP, kako se provodi Provedbenom odlukom Vijeća (ZVSP) 2023/1780, i u Uredbi Vijeća (EU) br. 359/2011, kako se provodi Provedbenom uredbom Vijeća (EU) 2023/1779, o mjerama ograničavanja protiv određenih osoba, subjekata i tijela s obzirom na stanje u Iranu	11
2023/C 328/04	Obavijest namijenjena ispitanicima na koje se primjenjuju mjere ograničavanja predviđene u Odluci Vijeća 2011/235/ZVSP i Uredbi Vijeća (EU) br. 359/2011 o mjerama ograničavanja protiv određenih osoba, subjekata i tijela s obzirom na stanje u Iranu	13

⁽¹⁾ Tekst značajan za EGP.

Europska komisija

2023/C 328/05	Sažetak odluka Europske komisije o autorizacijama za stavljanje na tržište radi uporabe i/ili za uporabu tvari navedenih u Prilogu XIV. Uredbi (EZ) br. 1907/2006 Europskog parlamenta i Vijeća o registraciji, evaluaciji, autorizaciji i ograničavanju kemikalija (REACH) (<i>Objavljeno na temelju članka 64. stavka 9. Uredbe (EZ) br. 1907/2006</i>) ⁽¹⁾ 15	15
2023/C 328/06	Tečajna lista eura – 15. rujna 2023. 16	16

V. Objave

POSTUPCI U VEZI S PROVEDBOM POLITIKE TRŽIŠNOG NATJECANJA

Europska komisija

2023/C 328/07	Prethodna prijava koncentracije (Predmet M.11239 – EDF / CREDIT MUTUEL / ILE-DE-FRANCE BUILDING) – Predmet primjeren za primjenu pojednostavnjenog postupka ⁽¹⁾ 17	17
---------------	---	----

⁽¹⁾ Tekst značajan za EGP.

II.

(Informacije)

INFORMACIJE INSTITUCIJA, TIJELA, UREDA I AGENCIJA EUROPSKE UNIJE

EUROPSKA KOMISIJA

Neprotivljenje prijavljenoj koncentraciji**(Predmet M.11106 – STELLANTIS / MICHELIN / FORVIA / SYMBIO)****(Tekst značajan za EGP)**

(2023/C 328/01)

Dana 17. srpnja 2023. Komisija je donijela odluku da se ne protivi prethodno spomenutoj prijavljenoj koncentraciji te je ocijenila da je ona sukladna s unutarnjim tržištem. Odluka se temelji na članku 6. stavku 1. točki (b) Uredbe Vijeća (EZ) br. 139/2004 ⁽¹⁾. Puni tekst odluke dostupan je samo na engleskom jeziku, a objavit će se nakon što se iz njega uklone sve moguće poslovne tajne. Odluka će biti dostupna:

- na internetskoj stranici Komisije posvećenoj tržišnom natjecanju, u odjeljku za koncentracije (<https://competition-cases.ec.europa.eu/search>). Odluke o spajanju mogu se pretraživati na različite načine, među ostalim po trgovačkom društvu, broju predmeta, datumu i sektoru,
- u elektroničkom obliku na internetskoj stranici EUR-Lexa (<http://eur-lex.europa.eu/homepage.html?locale=hr>) pod brojem dokumenta 32023M11106. EUR-Lex omogućuje mrežni pristup pravnim dokumentima Europske unije.

⁽¹⁾ SL L 24, 29.1.2004., str. 1.

KOMUNIKACIJA KOMISIJE**Smjernice Komisije za primjenu članka 4. stavaka 1. i 2. Direktive (EU) 2022/2555 (Direktiva NIS 2)**

(2023/C 328/02)

I. UVOD

1. U skladu s člankom 4. stavkom 3. Direktive (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije (Direktiva NIS 2) ⁽¹⁾ Komisija mora do 17. srpnja 2023. pružiti smjernice kojima se pojašnjava primjena članka 4. stavaka 1. i 2. te direktive.
2. U ovim se Smjernicama pojašnjava primjena tih odredbi o odnosu između Direktive (EU) 2022/2555 i postojećih i budućih sektorskih pravnih akata Unije koji se odnose na mjere upravljanja kibernetičkim sigurnosnim rizicima ili zahtjeve za izvješćivanje o incidentima. U dodatku Smjernicama navedeni su sektorski pravni akti Unije za koje Komisija smatra da su obuhvaćeni područjem primjene članka 4. Direktive (EU) 2022/2555. Ako akt nije naveden u tom dodatku, to ne znači nužno da nije obuhvaćen područjem primjene te odredbe.
3. Primjenjujući članak 4. stavak 3. treću rečenicu Direktive (EU) 2022/2555, Komisija je prije donošenja ovih Smjernica uzela u obzir primjedbe Skupine za suradnju u području sigurnosti mrežnih i informacijskih sustava i Agencije Europske unije za kibersigurnost (ENISA).
4. Ovim se Smjernicama ne dovodi u pitanje način na koji Sud Europske unije tumači pravo Unije.

II. JEDNAKOVRIJEDNOST KIBERNETIČKIH SIGURNOSNIH ZAHTEJEVA SEKTORSKIH PRAVNIH AKATA UNIJE

5. Člankom 4. stavkom 1. Direktive (EU) 2022/2555 propisuje se da se, ako se sektorskim pravnim aktima Unije od ključnih ili važnih subjekata zahtijeva donošenje mjera upravljanja kibernetičkim sigurnosnim rizicima ili obavješćivanje o značajnim incidentima i ako su ti zahtjevi po učinku barem jednakovrijedni obvezama utvrđenima u toj direktivi, relevantne odredbe te direktive, uključujući odredbe o nadzoru i izvršavanju iz poglavlja VII., ne primjenjuju na te subjekte. Tom se odredbom propisuje i da se, ako sektorski pravni akti Unije ne obuhvaćaju sve subjekte u određenom sektoru koji su obuhvaćeni područjem primjene Direktive (EU) 2022/2555, relevantne odredbe te direktive i dalje primjenjuju na subjekte koji nisu obuhvaćeni tim sektorskim pravnim aktima Unije.

II.1. Zahtjevi za upravljanje kibernetičkim sigurnosnim rizicima

6. Člankom 4. stavkom 2. točkom (a) Direktive (EU) 2022/2555 propisuje se da se mjere upravljanja kibernetičkim sigurnosnim rizicima koje su ključni ili važni subjekti dužni donijeti na temelju sektorskih pravnih akata Unije smatraju po učinku jednakovrijednima obvezama utvrđenima u toj direktivi ako su po učinku barem jednakovrijedne onima utvrđenima u članku 21. stavcima 1. i 2. te direktive. Pri procjeni jesu li zahtjevi u pogledu mjera upravljanja kibernetičkim sigurnosnim rizicima iz sektorskog pravnog akta Unije po učinku barem jednakovrijedni onima iz članka 21. stavaka 1. i 2. Direktive (EU) 2022/2555, zahtjevi iz tog sektorskog pravnog akta Unije trebali bi barem odgovarati zahtjevima tih odredbi ili ih nadilaziti, što znači da sadržaj sektorskih odredbi može biti iscrpniji u usporedbi s odgovarajućim odredbama Direktive (EU) 2022/2555.

(1) SL L 333, 27.12.2022., str. 80.

7. U skladu s člankom 21. stavkom 1. prvim podstavkom Direktive (EU) 2022/2555 države članice osiguravaju da ključni i važni subjekti poduzimaju odgovarajuće i razmjerne tehničke, operativne i organizacijske mjere za upravljanje rizicima kojima su izloženi mrežni i informacijski sustavi kojima se ti subjekti služe u svojem poslovanju ili u pružanju svojih usluga. Te mjere trebale bi se temeljiti na procjeni rizika i trebale bi moći spriječiti učinak incidenata ili ga svesti na najmanju moguću mjeru. U članku 21. stavku 1. drugom podstavku Direktive (EU) 2022/2555 utvrđuje se kako bi trebalo procjenjivati proporcionalnost takvih mjera^(?). Obveza utvrđena u članku 21. stavku 1. Direktive (EU) 2022/2555, kojom se propisuje da su ključni i važni subjekti dužni poduzimati odgovarajuće i razmjerne tehničke, operativne i organizacijske mjere za upravljanje kibernetičkim sigurnosnim rizicima, odnosi se na sve djelatnosti i usluge predmetnog subjekta, a ne samo na određenu informatičku imovinu ili kritične usluge koje subjekt pruža.
8. Pri procjeni jednakovrijednosti sektorskog pravnog akta Unije i relevantnih odredbi Direktive (EU) 2022/2555 o upravljanju kibernetičkim sigurnosnim rizicima posebnu važnost trebalo bi pridati pitanju obuhvaćaju li sigurnosne obveze iz tog pravnog akta mjere čiji je cilj zajamčiti sigurnost mrežnih i informacijskih sustava. Definicija pojma „sigurnost mrežnih i informacijskih sustava” iz članka 6. točke 2. Direktive (EU) 2022/2555 odnosi se na sposobnost mrežnih i informacijskih sustava da na određenoj razini pouzdanosti odolijevaju svim događajima koji mogu ugroziti dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili usluga koje ti mrežni i informacijski sustavi nude ili kojima omogućuju pristup. Upotreba pojmova „dostupnost”, „autentičnost”, „cjelovitost” i „povjerljivost” u toj definiciji odnosi se na sva četiri cilja zaštite povezana sa sigurnošću mrežnih i informacijskih sustava. Pojam „mrežni i informacijski sustav”, kako je definiran u članku 6. točki 1. Direktive (EU) 2022/2555, obuhvaća elektroničke komunikacijske mreže⁽³⁾, svaki uređaj ili skupinu povezanih ili srodnih uređaja, od kojih jedan ili više njih programski izvršava automatsku obradu digitalnih podataka i digitalne podatke koji se pohranjuju, obrađuju, dobivaju ili prenose takvim elektroničkim komunikacijskim mrežama ili uređajima u svrhu njihova rada, uporabe, zaštite ili održavanja. Stoga bi sigurnosne mjere koje se propisuju sektorskim pravnim aktom Unije trebale obuhvaćati i hardver, integrirani softver i softver koji određeni subjekt upotrebljava u okviru svoje djelatnosti.
9. Pri procjeni jednakovrijednosti sektorskog pravnog akta Unije i zahtjeva iz članka 21. stavaka 1. i 2. Direktive (EU) 2022/2555 treba uzeti u obzir i činjenicu da bi se mjere upravljanja kibernetičkim sigurnosnim rizicima koje se propisuju tim aktom trebale temeljiti na pristupu kojim se uzimaju u obzir sve opasnosti. Budući da prijetnje sigurnosti mrežnih i informacijskih sustava mogu biti različitog podrijetla, bilo koja vrsta događaja može negativno utjecati na mrežne i informacijske sustave subjekta i potencijalno dovesti do incidenta. Stoga bi mjere upravljanja kibernetičkim sigurnosnim rizicima koje subjekt poduzima trebale štiti mrežne i informacijske sustave, ali i fizičko okruženje tih sustava od događaja kao što su sabotaza, krađa, požar, poplava, prekid u telekomunikacijama ili prekid opskrbe električnom energijom ili od bilo kojeg neovlaštenog fizičkog pristupa koji bi mogli ugroziti dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili usluga koje se nude ili kojima se pristupa putem mrežnih i informacijskih sustava. Mjere upravljanja kibernetičkim sigurnosnim rizicima propisane sektorskim pravnim aktom Unije trebale bi se stoga posebno odnositi na fizičku sigurnost i sigurnost okruženja mrežnih i informacijskih sustava od kvarova u sustavu, ljudske pogreške, zlonamjernih radnji ili prirodnih pojava⁽⁴⁾.
10. Nadalje, člankom 21. stavkom 2. Direktive (EU) 2022/2555 zahtijeva se da mjere upravljanja kibernetičkim sigurnosnim rizicima uključuju posebne sigurnosne zahtjeve navedene u točkama od (a) do (j) tog stavka. Ti zahtjevi obuhvaćaju mjere kao što su politike analize rizika i sigurnosti informacijskih sustava, postupanje s incidentima, kontinuitet poslovanja, sigurnost lanca opskrbe te politike i postupke u pogledu kriptografije i, prema potrebi, kriptiranja. U skladu s člankom 21. stavkom 5. drugim podstavkom Direktive (EU) 2022/2555 Komisija je ovlaštena donositi provedbene akte kojima se utvrđuju tehnički i metodološki zahtjevi te, prema potrebi, sektorski zahtjevi za sigurnosne mjere iz članka 21. stavka 2. te direktive. Kad je riječ o pružateljima usluga sustava naziva

^(?) Vidjeti i uvodne izjave 78., 81. i 82. Direktive (EU) 2022/2555.

⁽³⁾ Članak 2. točka 1. Direktive (EU) 2018/1972 Europskog parlamenta i Vijeća od 11. prosinca 2018. o Europskom zakoniku elektroničkih komunikacija (SL L 321, 17.12.2018., str. 36.).

⁽⁴⁾ Vidjeti uvodnu izjavu 79. Direktive (EU) 2022/2555.

domena („DNS”), registrima naziva vršnih domena („TLD”), pružateljima usluga računalstva u oblaku, pružateljima usluga podatkovnog centra, pružateljima mreža za isporuku sadržaja, pružateljima upravljanih usluga, pružateljima upravljanih sigurnosnih usluga, pružateljima internetskih tržišta, pružateljima internetskih tražilica, pružateljima platformi za usluge društvenih mreža i pružateljima usluga povjerenja, Komisija mora do 17. listopada 2024. donijeti provedbene akte o tehničkim i metodološkim zahtjevima za sigurnosne mjere iz članka 21. stavka 2. Direktive (EU) 2022/2555. U provedbenim aktima podrobnije se određuju glavni uvjeti i kriteriji za provedbu u skladu s odredbama iz temeljnog akta, a da se pritom ne utječe na njegov sadržaj ⁽⁹⁾.

II.2. Zahtjevi za izvješćivanje

11. Člankom 4. stavkom 2. točkom (b) Direktive (EU) 2022/2555 propisano je da se zahtjevi za izvješćivanje koji se odnose na obavješćivanje o značajnim incidentima smatraju po učinku jednakovrijednima obvezama iz te direktive ako se sektorskim pravnim aktom Unije predviđa neposredan, prema potrebi automatski i izravan, pristup obavijestima o incidentima od strane timova za odgovor na računalne sigurnosne incidente (CSIRT), nadležnih tijela ili jedinstvenih kontaktnih točaka te ako su zahtjevi za obavješćivanje o značajnim incidentima po učinku barem jednakovrijedni onima iz članka 23. stavaka od 1. do 6. te direktive.
12. Budući da zahtjevi za obavješćivanje o značajnim incidentima iz sektorskog pravnog akta Unije moraju po učinku biti barem jednakovrijedni onima iz članka 23. stavaka 1. i 6. Direktive (EU) 2022/2555 kako bi se taj akt primjenjivao umjesto obveza izvješćivanja iz te direktive, zahtjevi iz članka 23. stavaka od 1. do 6. Direktive osobito su važni za procjenu jednakovrijednosti. U članku 23. stavcima od 1. do 6. Direktive (EU) 2022/2555 podrobnije se određuje koga se i u kojem vremenskom okviru mora obavijestiti o kojem incidentu i koje je informacije potrebno dostaviti. To je detaljnije objašnjeno u sljedećim pododjeljcima.

II.2.1. Obavješćivanje CSIRT-ova, nadležnih tijela i primatelja o značajnim incidentima

13. U članku 23. stavku 1. prvom podstavku prvoj rečenici Direktive (EU) 2022/2555 propisuje se da su ključni i važni subjekti o svakom značajnom incidentu bez nepotrebne odgode dužni obavijestiti svoj CSIRT ili, ako je to primjenjivo, svoje nadležno tijelo. U članku 23. stavku 1. prvom podstavku drugoj rečenici Direktive (EU) 2022/2555 propisuje se da su ključni i važni subjekti prema potrebi dužni bez nepotrebne odgode obavijestiti primatelje svojih usluga o značajnim incidentima koji bi mogli negativno utjecati na pružanje tih usluga.
14. Iako su u članku 6. točki 6. Direktive (EU) 2022/2555 „incidenti” definirani vrlo široko kao svi događaji koji ugrožavaju dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili usluga koje mrežni i informacijski sustavi nude ili kojima omogućuju pristup, prema članku 23. stavku 1. te direktive obveza izvješćivanja primjenjuje se samo na značajne incidente. Incident je značajan ako je uzrokovao ili može uzrokovati ozbiljne poremećaje u funkcioniranju usluga ili financijske gubitke za predmetni subjekt (članak 23. stavak 3. točka (a)) ili ako je utjecao ili bi mogao utjecati na druge fizičke ili pravne osobe uzrokovanjem znatne materijalne ili nematerijalne štete (članak 23. stavak 3. točka (b)).

⁽⁹⁾ Vidjeti poglavlje D (Dodatna pravila kojima se provodi temeljni akt) Neobvezujućih kriterija za primjenu članaka 290. i 291. Ugovora o funkcioniranju Europske unije – 18. lipnja 2019. (SL C 223, 3.7.2019., str. 1.).

15. U uvodnoj izjavi 101. Direktive (EU) 2022/2555 pojašnjava se da bi se izvješćivanje o incidentima trebalo temeljiti na početnoj procjeni koju provodi predmetni subjekt. Takvom početnom procjenom trebalo bi uzeti u obzir, među ostalim, pogođene mrežne i informacijske sustave, a posebno njihovu važnost u pružanju usluga predmetnog subjekta, ozbiljnost i tehničke značajke kibernetičke prijetnje te sve temeljne ranjivosti koje se iskorištavaju, kao i iskustvo subjekta sa sličnim incidentima. Pokazatelji kao što su mjera u kojoj je ugroženo funkcioniranje usluge, trajanje incidenta ili broj primatelja usluga na koje je incident utjecao mogli bi imati važnu ulogu u utvrđivanju je li poremećaj u funkcioniranju usluge ozbiljan.
16. U skladu s člankom 23. stavkom 11. drugim podstavkom Direktive (EU) 2022/2555 Komisija je ovlaštena donijeti provedbene akte kojima se dodatno utvrđuju slučajevi u kojima se incident smatra značajnim. U pogledu pružatelja usluga sustava naziva domena (DNS), registara naziva vršnih domena, pružatelja usluga računalstva u oblaku, pružatelja usluga podatkovnog centra, pružatelja mreža za isporuku sadržaja, pružatelja upravljanih usluga, pružatelja upravljanih sigurnosnih usluga, pružatelja internetskih tržišta, pružatelja internetskih tražilica i pružatelja platformi za usluge društvenih mreža Komisija takve provedbene akte donosi do 17. listopada 2024. U provedbenim aktima podrobnije se određuju glavni uvjeti i kriteriji za provedbu u skladu s odredbama iz temeljnog akta, a da se pritom ne utječe na njegov sadržaj ⁽⁶⁾.

II.2.2. *Pristup izvješćivanju o značajnim incidentima u više faza i vremenski okvir za takvo izvješćivanje*

17. Direktivom (EU) 2022/2555 propisuje se pristup izvješćivanju o značajnim incidentima u više faza koji obuhvaća rano upozorenje, obavijest o incidentu i završno izvješće. Ta se tri elementa mogu dopuniti privremenim izvješćima i izvješćem o napretku.
18. Pristupom izvješćivanju o značajnim incidentima u više faza nastoji se uspostaviti prava ravnoteža između, s jedne strane, brzog izvješćivanja koje doprinosi ublažavanju potencijalnog širenja značajnih incidenata i omogućuje ključnim i važnim subjektima da zatraže podršku te, s druge strane, detaljnog izvješćivanja kojim se iz pojedinačnih incidenata izvlače vrijedne pouke i s vremenom poboljšava otpornost pojedinačnih subjekata i cijelih sektora na kibernetičke prijetnje ⁽⁷⁾.
19. U skladu s pristupom u više faza ključni i važni subjekti prvo bez nepotrebne odgode, a u svakom slučaju u roku od 24 sata od kad su saznali za značajan incident, nadležnom CSIRT-u ili tijelu moraju podnijeti rano upozorenje. Potom bez nepotrebne odgode, a u svakom slučaju u roku od 72 sata od kad su saznali za značajan incident, moraju podnijeti obavijest o incidentu. Nadležni CSIRT ili nadležno tijelo nakon toga može zatražiti privremeno izvješće. Konačno, nadležnom CSIRT-u ili tijelu mora se najkasnije mjesec dana nakon podnošenja obavijesti o incidentu dostaviti završno izvješće, osim ako je incident u tom trenutku još uvijek u tijeku. U tom slučaju mora se dostaviti izvješće o napretku, a završno izvješće dostavlja se u roku od mjesec dana od postupanja s incidentom.
20. Za pružatelje usluga povjerenja vrijedi drukčiji vremenski okvir za podnošenje obavijesti o incidentu, koji je utvrđen u članku 23. stavku 4. drugom podstavku Direktive (EU) 2022/2555. Oni obavijest o značajnim incidentima s učinkom na pružanje njihovih usluga povjerenja moraju podnijeti bez nepotrebne odgode, a u svakom slučaju u roku od 24 sata od kad su saznali za značajan incident.

⁽⁶⁾ Vidjeti poglavlje D (Dodatna pravila kojima se provodi temeljni akt) Neobvezujućih kriterija za primjenu članaka 290. i 291. Ugovora o funkcioniranju Europske unije – 18. lipnja 2019. (SL C 223, 3.7.2019., str. 1.).

⁽⁷⁾ Vidjeti uvodnu izjavu 101. Direktive (EU) 2022/2555.

II.2.3. Sadržaj obveze izvješćivanja CSIRT-ova ili nadležnih tijela o značajnim incidentima

21. Kao opće pravilo člankom 23. stavkom 1. prvim podstavkom trećom rečenicom Direktive (EU) 2022/2555 propisuje se da su države članice dužne osigurati da ključni i važni subjekti dostavljaju, među ostalim, sve informacije koje nadležnom CSIRT-u ili, ako je to primjenjivo, nadležnom tijelu omogućuju da utvrde sve prekogranične učinke incidenta. Taj zahtjev u pogledu sadržaja obveze izvješćivanja detaljnije je razložen u članku 23. stavku 4. Direktive (EU) 2022/2555, u kojem se utvrđuje pristup u više faza.
22. U skladu s člankom 23. stavkom 4. točkom (a) u ranom upozorenju mora se, ako je to primjenjivo, naznačiti postoji li sumnja da je značajan incident uzrokovan nezakonitim ili zlonamjernim djelovanjem te bi li mogao imati prekogranični učinak (tj. postoji li vjerojatnost da će ga imati). Prema uvodnoj izjavi 102. Direktive (EU) 2022/2555 rano upozorenje trebalo bi sadržavati samo informacije koje su nužne kako bi CSIRT ili, ako je to primjenjivo, nadležno tijelo bili upoznati sa značajnim incidentom i kako bi se dotičnom subjektu prema potrebi omogućilo traženje pomoći.
23. Ako je to primjenjivo, u obavijesti o incidentu moraju se ažurirati informacije dostavljene u ranom upozorenju. Usto, u njoj se moraju navesti početna procjena značajnog incidenta, uključujući njegovu ozbiljnost i učinak te, ako su dostupni, pokazatelji ugroženosti.
24. Ako se zatraži privremeno izvješće, ono mora sadržavati relevantna ažuriranja statusa. Završno izvješće mora sadržavati detaljan opis incidenta, uključujući njegovu ozbiljnost i učinak, vrstu prijetnje ili temeljni uzrok koji je vjerojatno uzrokovao incident, primijenjene i tekuće mjere ublažavanja i, ako je to primjenjivo, prekogranični učinak incidenta.

II.2.4. Neposredan pristup obavijestima o incidentima

25. Člankom 4. stavkom 2. točkom (b) Direktive (EU) 2022/2555 propisano je da se na zahtjeve za izvješćivanje umjesto te direktive može primjenjivati sektorski pravni akt Unije ako se njime CSIRT-ovima, nadležnim tijelima ili jedinstvenim kontaktnim točkama iz Direktive (EU) 2022/2555 omogućuje neposredan pristup obavijestima o incidentima dostavljenima u skladu s tim sektorskim pravnim aktom Unije. U skladu s uvodnom izjavom 24. Direktive (EU) 2022/2555 takav se neposredan pristup konkretno može osigurati ako se obavijesti o incidentima bez nepotrebne odgode prosljeđuju CSIRT-u, nadležnom tijelu ili jedinstvenoj kontaktnoj točki.
26. Neposredan pristup može se omogućiti automatskim i izravnim sredstvima koje bi prema potrebi trebale uspostaviti države članice. Mehanizmi automatskog i izravnog izvješćivanja omogućuju sustavnu i neposrednu razmjenu informacija s CSIRT-ovima, nadležnim tijelima ili jedinstvenim kontaktnim točkama o postupanju s obavijestima o incidentima. U cilju pojednostavnjenja izvješćivanja i uspostave mehanizma automatskog i izravnog izvješćivanja države članice također mogu upotrebljavati jedinstvenu ulaznu točku koja mora biti u skladu sa sektorskim pravnim aktom Unije.
27. Pri procjeni jesu li zahtjevi za obavješćivanje o značajnim incidentima iz sektorskog pravnog akta Unije po učinku barem jednakovrijedni onima iz članka 23. stavaka od 1. do 6. Direktive (EU) 2022/2555, zahtjevi iz tog sektorskog pravnog akta Unije trebali bi barem odgovarati zahtjevima iz članka 23. stavaka od 1. do 6. ili biti detaljniji od tih odredbi. Zahtjevi bi se trebali odnositi na vrstu incidenata koje je potrebno prijaviti u skladu s Direktivom (EU) 2022/2555, pri čemu posebno treba voditi računa o primateljima, sadržaju i predviđenim vremenskim okvirima.

III. POSLJEDICE JEDNAKOVRIJEDNOSTI

III.1. Nadzor i izvršavanje

28. Ako su sektorski pravni akti Unije po učinku barem jednakovrijedni obvezama utvrđenima u Direktivi (EU) 2022/2555, ne primjenjuju se ni relevantne odredbe te direktive koje se odnose na obvezu donošenja mjera upravljanja kibernetičkim sigurnosnim rizicima ili obavješćivanja o značajnim incidentima ni odredbe o nadzoru i izvršavanju iz poglavlja VII. te direktive.
29. U uvodnoj izjavi 25. Direktive (EU) 2022/2555 objašnjava se da bi se sektorskim pravnim aktima Unije koji su po učinku barem jednakovrijedni moglo propisati da nadležna tijela na temelju takvih akata svoje nadzorne ovlasti i ovlasti izvršavanja u vezi s mjerama upravljanja kibernetičkim sigurnosnim rizicima ili obvezama izvješćivanja izvršavaju uz pomoć nadležnih tijela na temelju te direktive. Predmetna nadležna tijela mogla bi u tu svrhu uspostaviti dogovore o suradnji, uključujući postupke koji se odnose na koordinaciju nadzornih aktivnosti, postupke istraga i inspekcije na lokaciji u skladu s nacionalnim pravom te mehanizam za razmjenu relevantnih informacija o nadzoru i izvršavanju među nadležnim tijelima. Takav mehanizam za razmjenu relevantnih informacija mogao bi uključivati pristup informacijama povezanim s kibernetičkom sigurnošću koje nadležna tijela zahtijevaju na temelju Direktive (EU) 2022/2555.

III.2. Nacionalna strategija za kibernetičku sigurnost

30. Svaka država članica je u skladu s člankom 7. stavkom 1. Direktive (EU) 2022/2555 dužna donijeti nacionalnu strategiju za kibernetičku sigurnost. Nacionalna strategija za kibernetičku sigurnost je koherentan okvir države članice kojim se predviđaju strateški ciljevi i prioritete u području kibernetičke sigurnosti i upravljanje za njihovo postizanje u toj državi članici (vidjeti članak 6. točku 4. Direktive (EU) 2022/2555). Strategija za kibernetičku sigurnost mora uključivati, među ostalim, ciljeve i prioritete koji posebno obuhvaćaju sektore i podsektore iz priloga I. i II. Direktivi (EU) 2022/2555. Usto, ta strategija mora uključivati upravljački okvir za postizanje tih ciljeva i prioriteta, uključujući politike iz članka 7. stavka 2. Direktive (EU) 2022/2555.
31. Nadalje, člankom 7. stavkom 1. točkom (c) Direktive (EU) 2022/2555 propisuje se da nacionalna strategija za kibernetičku sigurnost mora uključivati upravljački okvir kojim se pojašnjavaju uloge i odgovornosti relevantnih dionika na nacionalnoj razini te kojim se podupire suradnja i koordinacija na nacionalnoj razini među nadležnim tijelima, jedinstvenim kontaktnim točkama i CSIRT-ovima na temelju te direktive, kao i koordinacija i suradnja između tih tijela i nadležnih tijela na temelju sektorskih pravnih akata Unije.
32. Dakle, zahtjev za donošenje strategije za kibernetičku sigurnost u skladu s člankom 7. Direktive (EU) 2022/2555 ne odnosi se ni na kibernetičke sigurnosne zahtjeve koje moraju ispunjavati ključni i važni subjekti u skladu s člancima 21. i 23. te direktive ni na odredbe koje se odnose na njihov nadzor i izvršavanje iz poglavlja VII. kako je propisano člankom 4. stavcima 1. i 2. te direktive. Relevantna odredba iz članka 7. i dalje bi se trebala primjenjivati na sektore, podsektore i vrste subjekata za koje postoje sektorski pravni akti Unije u smislu članka 4. Direktive (EU) 2022/2555.

III.3. Imenovanje CSIRT-ova

33. U skladu s člankom 10. stavkom 1. Direktive (EU) 2022/2555 države članice moraju imenovati ili uspostaviti jedan ili više CSIRT-ova koji obuhvaćaju barem sektore, podsektore ili vrste subjekata iz priloga I. i II. Direktive, što uključuje sektore, podsektore i vrste subjekata za koje postoje sektorski pravni akti Unije. CSIRT-ovi će u tom pogledu u pravilu obavljati i svoje zadaće iz članka 11. stavka 3. Direktive (EU) 2022/2555, osim ako su u sektorskim pravnim aktima Unije navedene posebne zadaće.

III.4. Nacionalni okviri za upravljanje kibernetičkim krizama i EU-CyCLONe

34. U skladu s člankom 9. stavkom 1. Direktive (EU) 2022/2555 države članice moraju imenovati ili uspostaviti jedno ili više nadležnih tijela odgovornih za upravljanje kibernetičkim sigurnosnim incidentima velikih razmjera i krizama. U skladu s člankom 6. točkom 7. te direktive kibernetički sigurnosni incident velikih razmjera je incident koji uzrokuje razinu poremećaja koja premašuje sposobnost države članice da na njega odgovori ili koji ima znatan učinak na najmanje dvije države članice. Člankom 9. stavkom 4. Direktive (EU) 2022/2555 od država članica zahtijeva se i da donesu nacionalni plan za odgovor na kibernetičke sigurnosne incidente velikih razmjera i krize u kojem se utvrđuju ciljevi i načini upravljanja kibernetičkim sigurnosnim incidentima velikih razmjera i krizama. U tom planu trebalo bi, među ostalim, utvrditi postupke upravljanja kibernetičkim krizama, uključujući njihovu integraciju u opći nacionalni okvir za upravljanje krizama, i kanale za razmjenu informacija te relevantne javne i privatne dionike i uključenu infrastrukturu. Takvi postupci upravljanja kibernetičkim krizama te relevantni javni i privatni dionici i infrastruktura mogu uključivati sektorske postupke i dionike.
35. Člankom 16. Direktive (EU) 2022/2555 uspostavlja se Europska mreža organizacija za vezu za kibernetičke krize (EU-CyCLONe), čija je svrha podržati koordinirano upravljanje kibernetičkim sigurnosnim incidentima velikih razmjera i krizama na operativnoj razini i osigurati redovitu razmjenu relevantnih informacija među državama članicama te institucijama, tijelima i agencijama Unije.
36. Budući da se članak 9. o okvirima za upravljanje kibernetičkim krizama i članak 16. o mreži EU-CyCLONe ne odnose na kibernetičke sigurnosne zahtjeve koje subjekti moraju ispunjavati u skladu s člancima 21. i 23. Direktive (EU) 2022/2555 ni na nadzor i izvršavanje iz poglavlja VII. kako je propisano člankom 4. stavcima 1. i 2. te direktive, članci 9. i 16. trebali bi se na sektore primjenjivati u cijelosti unatoč postojanju sektorskih pravnih akata Unije u smislu članka 4. Zbog toga države članice moraju imenovati ili uspostaviti jedno ili više nadležnih tijela odgovornih za upravljanje kibernetičkim sigurnosnim incidentima velikih razmjera i krizama koje se događaju u sektorima obuhvaćenima sektorskim pravnim aktima Unije. Nadalje, pri donošenju nacionalnog plana za odgovor na kibernetičke sigurnosne incidente velikih razmjera i krize ne bi se smjeli zanemariti sektori obuhvaćeni sektorskim pravnim aktima Unije. Naposljetku, EU-CyCLONe svoje bi zadace utvrdile u članku 16. Direktive (EU) 2022/2555 trebao obavljati u pogledu sektora u kojima se na subjekte primjenjuju sektorski pravni akti Unije.

III.5. Isključenje iz primjene članka 3. stavaka 3. i 4., članka 20. i članka 27. stavaka 2. i 3.

37. U skladu s člankom 3. stavkom 3. Direktive (EU) 2022/2555 države članice dužne su utvrditi popis ključnih i važnih subjekata te subjekata koji pružaju usluge registracije naziva domena koji su obuhvaćeni područjem primjene Direktive. U skladu s člankom 27. stavkom 2. države članice moraju od subjekata iz članka 27. stavka 1. te direktive zatražiti da nadležnim tijelima dostavljaju određene informacije. Budući da je svrha tih odredbi osigurati jasan pregled subjekata obuhvaćenih područjem primjene Direktive (EU) 2022/2555 kako bi se podupro nadzor ključnih i važnih subjekata obuhvaćenih njezinim područjem primjene, te odredbe ne bi se trebale primjenjivati na subjekte na koje se u pogledu zahtjeva za upravljanje kibernetičkim sigurnosnim rizicima i zahtjeva za izvješćivanje o njima primjenjuje određeni sektorski pravni akt Unije. To ne sprečava države članice da takve subjekte uvrste na popis.

U skladu s člankom 20. stavkom 1. Direktive (EU) 2022/2555 upravljačka tijela ključnih i važnih subjekata dužna su odobriti mjere upravljanja kibernetičkim sigurnosnim rizicima koje su ti subjekti poduzeli radi usklađivanja s člankom 21. i nadgledati njegovu provedbu te se mogu smatrati odgovornima za povrede tog članka od strane subjekata. U skladu s člankom 20. stavkom 2. te direktive države članice osiguravaju da članovi upravljačkih tijela ključnih i važnih subjekata moraju pohađati osposobljavanja te potiču ključne i važne subjekte da slično osposobljavanje redovito nude svojim zaposlenicima kako bi stekli dovoljno znanja i vještina za prepoznavanje i procjenu praksi upravljanja kibernetičkim sigurnosnim rizicima i njihova učinka na usluge koje taj subjekt pruža. Budući da su obveze koje proizlaze iz članka 20. Direktive (EU) 2022/2555 neodvojivo povezane sa zahtjevima članka 21. te direktive, članak 20. ne bi se trebao primjenjivati na sektorske pravne akte Unije u smislu članka 4. te direktive koji se primjenjuju na zahtjeve za upravljanje kibernetičkim sigurnosnim rizicima.

DODATAK

Sektorski pravni akti Unije

Uredba (EU) 2022/2554 (Akt o digitalnoj operativnoj otpornosti) ⁽¹⁾

1. Člankom 1. stavkom 2. Uredbe (EU) 2022/2554 (Akt o digitalnoj operativnoj otpornosti, DORA) propisuje da se, kad je riječ o financijskim subjektima obuhvaćenima Direktivom (EU) 2022/2555 i odgovarajućim pravilima za njezino prenošenje u nacionalno zakonodavstvo, Uredba (EU) 2022/2554 smatra sektorskim pravnim aktom Unije za potrebe članka 4. Direktive (EU) 2022/2555. Ta se izjava odražava u uvodnoj izjavi 28. Direktive (EU) 2022/2555, u kojoj se navodi da bi DORA-u trebalo smatrati sektorskim pravnim aktom Unije u odnosu na tu direktivu u pogledu financijskih subjekata. Odredbe Uredbe (EU) 2022/2554 koje se odnose na upravljanje rizicima informacijskih i komunikacijskih tehnologija (IKT) (članak 6. i dalje), upravljanje IKT incidentima, a posebno na izvješćivanje o značajnim IKT incidentima (članak 17. i dalje) te na testiranje digitalne operativne otpornosti (članak 24. i dalje), mehanizme razmjene informacija (članak 25. i dalje) i IKT rizik treće strane (članak 28. i dalje) stoga se primjenjuju umjesto odredaba Direktive (EU) 2022/2555. Države članice stoga odredbe Direktive (EU) 2022/2555 koje se odnose na obveze upravljanja kibernetičkim sigurnosnim rizicima i izvješćivanja te nadzor i izvršavanje ne bi trebale primjenjivati na financijske subjekte obuhvaćene Uredbom (EU) 2022/2554.
2. Financijskim subjektima u tom se pogledu smatraju subjekti iz članka 2. stavka 1. točaka od (a) do (t) Uredbe (EU) 2022/2554. Kreditne institucije, mjesta trgovanja i središnje druge ugovorne strane među onim su subjektima koji su obuhvaćeni područjem primjene Uredbe (EU) 2022/2554 kao financijski subjekti i područjem primjene Direktive (EU) 2022/2555 kao ključni ili važni subjekti. Budući da je važno očuvati čvrstu vezu i razmjenu informacija s financijskim sektorom na temelju Direktive (EU) 2022/2555, europska nadzorna tijela i nadležna tijela na temelju Uredbe (EU) 2022/2554 mogu zatražiti sudjelovanje u aktivnostima skupine za suradnju ⁽²⁾ te razmjenu informacija i suradnju s jedinstvenim kontaktnim točkama, CSIRT-ovima i nadležnim tijelima na temelju Direktive (EU) 2022/2555 ⁽³⁾. Nadležna tijela na temelju Uredbe (EU) 2022/2554 trebala bi također CSIRT-ovima, nadležnim tijelima ili jedinstvenim kontaktnim točkama na temelju Direktive (EU) 2022/2555 trebala slati podatke o značajnim IKT incidentima i, ako je to relevantno, ozbiljnim kibernetičkim prijetnjama. To se može postići pružanjem neposrednog pristupa obavijestima o incidentima i prosljeđivanjem tih obavijesti bilo izravno ili putem jedinstvene ulazne točke. CSIRT-ovi bi trebali moći svojim aktivnostima obuhvatiti financijski sektor ⁽⁴⁾. Države članice trebale bi nastaviti uključivati financijski sektor u svoje strategije za kibernetičku sigurnost. Odredbe o nacionalnim okvirima za upravljanje kibernetičkim krizama (članak 9. Direktive (EU) 2022/2555) i o mreži EU-CyCLONe (članak 16. Direktive (EU) 2022/2555) trebale bi se nastaviti primjenjivati na subjekte obuhvaćene područjem primjene Uredbe (EU) 2022/2554.

⁽¹⁾ Uredba (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 (SL L 333, 27.12.2022., str. 1.).

⁽²⁾ Članak 14. stavak 3. Direktive (EU) 2022/2555 i članak 47. stavak 1. Uredbe (EU) 2022/2554.

⁽³⁾ Vidjeti uvodnu izjavu 28. Direktive (EU) 2022/2555.

⁽⁴⁾ Isto.

IV.

(Obavijesti)

OBAVIJESTI INSTITUCIJA, TIJELA, UREDA I AGENCIJA EUROPSKE UNIJE

VIJEĆE EUROPSKE UNIJE

Obavijest osobama i subjektima na koje se primjenjuju mjere predviđene u Odluci Vijeća 2011/235/ZVSP, kako se provodi Provedbenom odlukom Vijeća (ZVSP) 2023/1780, i u Uredbi Vijeća (EU) br. 359/2011, kako se provodi Provedbenom uredbom Vijeća (EU) 2023/1779, o mjerama ograničavanja protiv određenih osoba, subjekata i tijela s obzirom na stanje u Iranu

(2023/C 328/03)

Osobama i subjektima koji su navedeni u Prilogu Odluci Vijeća 2011/235/ZVSP ⁽¹⁾, kako se provodi Provedbenom odlukom Vijeća (ZVSP) 2023/1780 ⁽²⁾, i u Prilogu I. Uredbi Vijeća (EU) br. 359/2011 ⁽³⁾, kako se provodi Provedbenom uredbom Vijeća (EU) 2023/1779 ⁽⁴⁾ o mjerama ograničavanja protiv određenih osoba, subjekata i tijela s obzirom na stanje u Iranu, skreće se pozornost na informacije navedene u nastavku.

Vijeće Europske unije odlučilo je da bi te osobe i subjekte trebalo uvrstiti na popis osoba i subjekata na koje se primjenjuju mjere ograničavanja iz Odluke 2011/235/ZVSP i Uredbe (EU) br. 359/2011.

Dotične osobe i subjekti obavješćuju se o mogućnosti podnošenja zahtjeva nadležnim tijelima odgovarajuće države članice (ili više njih), koja su navedena na internetskim stranicama iz Priloga II. Uredbi (EU) br. 359/2011, radi pribavljanja odobrenja za upotrebu zamrznutih sredstava za osnovne potrebe ili posebna plaćanja (usp. članak 4. Uredbe).

Dotične osobe i subjekti mogu do 1. siječnja 2024. Vijeću podnijeti zahtjev, zajedno s popratnom dokumentacijom, za ponovno razmatranje odluke o njihovu uvrštenju na navedeni popis, na sljedeću adresu:

Vijeće Europske unije
Glavno tajništvo
RELEX.1
Rue de la Loi 175/Wetstraat 175
1048 Bruxelles/Brussel
BELGIQUE/BELGIË

E-pošta: sanctions@consilium.europa.eu

⁽¹⁾ SL L 100, 14.4.2011., str. 51.

⁽²⁾ SL L 228 I, 15.9.2023., str. 6..

⁽³⁾ SL L 100, 14.4.2011., str. 1.

⁽⁴⁾ SL L 228 I, 15.9.2023., str. 1..

Dotične osobe i subjekti također se obavješćuju o mogućnosti osporavanja odluke Vijeća pred Općim sudom Europske unije, u skladu s uvjetima iz članka 275. drugog stavka i članka 263. četvrtog i šestog stavka Ugovora o funkcioniranju Europske unije.

Obavijest namijenjena ispitanicima na koje se primjenjuju mjere ograničavanja predviđene u Odluci Vijeća 2011/235/ZVSP i Uredbi Vijeća (EU) br. 359/2011 o mjerama ograničavanja protiv određenih osoba, subjekata i tijela s obzirom na stanje u Iranu

(2023/C 328/04)

U skladu s člankom 16. Uredbe (EU) 2018/1725 Europskog parlamenta i Vijeća ⁽¹⁾ ispitanicima se skreće pozornost na informacije navedene u nastavku.

Pravne osnove za taj postupak obrade čine Odluka Vijeća 2011/235/ZVSP ⁽²⁾, kako se provodi Provedbenom odlukom Vijeća (ZVSP) 2023/1780 ⁽³⁾, i Uredba Vijeća (EU) br. 359/2011 ⁽⁴⁾, kako se provodi Provedbenom uredbom Vijeća (EU) 2023/1779 ⁽⁵⁾.

Voditelj tog postupka obrade jest Vijeće Europske unije koje zastupa glavni direktor Glavne uprave za vanjske odnose (RELEX) Glavnog tajništva Vijeća, a služba zadužena za postupak obrade jest RELEX.1, s kojom se može stupiti u kontakt na adresi:

Vijeće Europske unije
Glavno tajništvo
RELEX.1
Rue de la Loi 175/Wetstraat 175
1048 Bruxelles/Brussel
BELGIQUE/BELGIË

E-adresa: <mailto:sanctions@consilium.europa.eu>

Sa službenikom Vijeća za zaštitu podataka može se stupiti u kontakt putem e-adrese:

Službenik za zaštitu podataka

<mailto:data.protection@consilium.europa.eu>

Svrha postupka obrade uspostava je i ažuriranje popisa osoba na koje se primjenjuju mjere ograničavanja u skladu s Odlukom 2011/235/ZVSP, kako se provodi Provedbenom odlukom Vijeća (ZVSP) 2023/1780, i Uredbom (EU) br. 359/2011, kako se provodi Provedbenom uredbom Vijeća (EU) 2023/1779.

Ispitanici su fizičke osobe koje ispunjavaju kriterije za uvrštenje na popis navedene u Odluci 2011/235/ZVSP i Uredbi (EU) br. 359/2011.

Prikupljeni osobni podaci obuhvaćaju podatke potrebne za ispravno utvrđivanje identiteta dotične osobe, obrazloženje i sve ostale podatke povezane s razlozima uvrštenja na popis.

Pravne osnove za obradu osobnih podataka čine odluke Vijeća donesene na temelju članka 29. UFEU-a i uredbe Vijeća donesene na temelju članka 215. UFEU-a u kojima se određuju fizičke osobe (ispitanici) i nalažu zamrzavanje imovine i ograničenja putovanja.

Obrada je nužna za izvršavanje zadaće od javnog interesa u skladu s člankom 5. stavkom 1. točkom (a) i za poštovanje pravnih obveza utvrđenih u prethodno navedenim pravnim aktima kojima voditelj obrade podliježe u skladu s člankom 5. stavkom 1. točkom (b) Uredbe (EU) 2018/1725.

Obrada je nužna zbog znatnog javnog interesa u skladu s člankom 10. stavkom 2. točkom (g) Uredbe (EU) 2018/1725.

Vijeće može dobiti osobne podatke ispitanika od država članica i/ili Europske službe za vanjsko djelovanje. Primatelji su osobnih podataka države članice, Europska komisija i Europska služba za vanjsko djelovanje.

⁽¹⁾ SL L 295, 21.11.2018., str. 39.

⁽²⁾ SL L 100, 14.4.2011., str. 51.

⁽³⁾ SL L 228 I, 15.9.2023., str. 6..

⁽⁴⁾ SL L 100, 14.4.2011., str. 1.

⁽⁵⁾ SL L 228 I, 15.9.2023., str. 1..

Svi osobni podaci koje Vijeće obrađuje u kontekstu samostalnih mjera ograničavanja EU-a ostat će pohranjeni pet godina od trenutka brisanja ispitanika s popisa osoba na koje se primjenjuje zamrzavanje imovine ili od trenutka isteka valjanosti mjere ili, ako je pokrenut sudski postupak pred Sudom, do donošenja konačne presude. Osobne podatke sadržane u dokumentima koje je registriralo Vijeće čuva Vijeće u svrhe arhiviranja u javnom interesu, u smislu članka 4. stavka 1. točke (e) Uredbe (EU) 2018/1725.

Vijeće će možda morati razmijeniti osobne podatke o ispitaniku s trećom zemljom ili međunarodnom organizacijom u kontekstu prijenosa uvrštenja na popis UN-a od strane Vijeća ili u kontekstu međunarodne suradnje u vezi s politikom mjera ograničavanja EU-a.

Ako ne postoji odluka o primjerenosti ili odgovarajuće zaštitne mjere, prijenos osobnih podataka trećoj zemlji ili međunarodnoj organizaciji temelji se na sljedećem uvjetu ili više njih, u skladu s člankom 50. Uredbe (EU) 2018/1725: prijenos je nužan iz važnih razloga od javnog interesa; prijenos je nužan za postavljanje, ostvarivanje ili obranu pravnih zahtjeva.

U obradu osobnih podataka ispitanika nije uključeno automatizirano donošenje odluka.

Ispitanici imaju pravo na informacije i pravo pristupa svojim osobnim podacima. Također imaju pravo na ispravak i dopunu svojih podataka. U određenim okolnostima mogu imati pravo na brisanje svojih osobnih podataka ili pravo prigovora na obradu svojih osobnih podataka ili mogu zatražiti njezino ograničenje.

Ispitanici mogu ostvariti ta prava slanjem e-poruke voditelju obrade, uz kopiju službeniku za zaštitu podataka, kako je prethodno navedeno.

Uz svoj zahtjev ispitanici moraju dostaviti presliku identifikacijske isprave kako bi potvrdili svoj identitet (osobna iskaznica ili putovnica). Ta isprava treba sadržavati identifikacijski broj, državu izdavanja, razdoblje valjanosti, ime, adresu i datum rođenja. Svi drugi podaci koje sadržava preslika identifikacijske isprave, poput fotografije ili osobnih obilježja, mogu se zacrniti.

Ispitanici imaju pravo podnijeti pritužbu Europskom nadzorniku za zaštitu podataka u skladu s Uredbom (EU) 2018/1725 (<mailto:edps@edps.europa.eu>).

Prije toga preporučuje se da ispitanici prvo pokušaju iskoristiti pravni lijek tako da se obrate voditelju obrade i/ili službeniku Vijeća za zaštitu podataka.

EUROPSKA KOMISIJA

Sažetak odluka Europske komisije o autorizacijama za stavljanje na tržište radi uporabe i/ili za uporabu tvari navedenih u Prilogu XIV. Uredbi (EZ) br. 1907/2006 Europskog parlamenta i Vijeća o registraciji, evaluaciji, autorizaciji i ograničavanju kemikalija (REACH)

(Objavljeno na temelju članka 64. stavka 9. Uredbe (EZ) br. 1907/2006 ⁽¹⁾)

(Tekst značajan za EGP)

(2023/C 328/05)

Odluka o povlačenju autorizacije

Upućivanje na odluku ⁽¹⁾	Datum odluke	Naziv tvari	Adresat odluke	Povučena uporaba	Odluka stavljena izvan snage	Obrazloženje odluke
C(2023) 6014	11. rujna 2023.	Natrijev dikromat EZ br. 234-190-3; CAS br. 10588-019 (bezvodni); CAS br. 7789-12-0 (dihidrat)	Gruppo Colle S.r.l., Via G. Di Vittorio 3/5, 59025 Usella, Cantagallo, Prato, Italija	Kao sredstvo za nagrizanje pri bojenju vune tamnim bojama	C(2017) 8331	U izvješću o preispitivanju nije dokazano da podnositelj zahtjeva ne raspolaže prikladnim alternativama u skladu s člankom 60. stavkom 4. Uredbe (EZ) br. 1907/2006.

⁽¹⁾ Odluka je dostupna na internetskim stranicama Europske komisije: Autorizacija (europa.eu).

⁽¹⁾ OJ L 396, 30.12.2006., str. 1.

Tečajna lista eura ⁽¹⁾**15. rujna 2023.**

(2023/C 328/06)

1 euro =

Valuta	Tečaj	Valuta	Tečaj		
USD	američki dolar	1,0658	CAD	kanadski dolar	1,4409
JPY	japanski jen	157,50	HKD	hongkonški dolar	8,3416
DKK	danska kruna	7,4573	NZD	novozelandski dolar	1,8008
GBP	funta sterlinga	0,85878	SGD	singapurski dolar	1,4524
SEK	švedska kruna	11,8730	KRW	južnokorejski von	1 415,78
CHF	švicarski franak	0,9554	ZAR	južnoafrički rand	20,2968
ISK	islandska kruna	145,30	CNY	kineski renminbi-juan	7,7561
NOK	norveška kruna	11,4220	IDR	indonezijska rupija	16 379,21
BGN	bugarski lev	1,9558	MYR	malezijski ringit	4,9922
CZK	češka kruna	24,496	PHP	filipinski pezo	60,612
HUF	mađarska forinta	383,75	RUB	ruski rubalj	
PLN	poljski zlot	4,6308	THB	tajlandski baht	38,145
RON	rumunjski novi leu	4,9698	BRL	brazilski real	5,1860
TRY	turska lira	28,7513	MXN	meksički pezo	18,2275
AUD	australski dolar	1,6498	INR	indijska rupija	88,6150

⁽¹⁾ Izvor: referentna tečajna lista koju objavljuje ESB.

V.

(Objave)

POSTUPCI U VEZI S PROVEDBOM POLITIKE TRŽIŠNOG NATJECANJA

EUROPSKA KOMISIJA

Prethodna prijava koncentracije

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

Predmet primjeren za primjenu pojednostavnjenog postupka

(Tekst značajan za EGP)

(2023/C 328/07)

1. Komisija je 8. rujna 2023. zaprimila prijavu predložene koncentracije u skladu s člankom 4. Uredbe Vijeća (EZ) br. 139/2004⁽¹⁾.

Ta se prijava odnosi na sljedeće poduzetnike:

- SAS C91 (Francuska), pod kontrolom poduzetnika Électricité de France („EDF”, Francuska),
- La Française Real Estate Managers („La Française”, Francuska), pod kontrolom poduzetnika Caisse Régionale Crédit Mutuel Nord Europe (Francuska), koji je sam član grupacije Crédit Mutuel (Francuska),
- Zgrada smještena u regiji Ile-de-France („Zgrada”, Francuska).

Poduzetnici EDF i Crédit Mutuel steći će, u smislu članka 3. stavka 1. točke (b) Uredbe o koncentracijama, zajedničku kontrolu nad cijelom Zgradom.

Koncentracija se provodi kupnjom imovine.

2. Poslovne su djelatnosti predmetnih poduzetnika sljedeće:

- EDF: poduzeće koje se u Francuskoj i inozemstvu bavi proizvodnjom i veleprodajom električne energije, prijenosom i distribucijom električne energije te opskrbom električnom energijom, pružanjem drugih usluga povezanih s električnom energijom i, u manjoj mjeri, proizvodnjom, veleprodajom i maloprodajom plina,
- Crédit Mutuel: bavi se pružanjem bankarskih i financijskih usluga, uglavnom u Francuskoj. Grupacija Crédit Mutuel preko svojeg društva kćeri La Française nudi usluge upravljanja nekretninama.

3. Zgrada je uredska i komercijalna zgrada smještena na adresi 111, avenue de France, 75013 Pariz, Francuska.

4. Preliminarnim ispitivanjem Komisija je ocijenila da bi prijavljena transakcija mogla biti obuhvaćena područjem primjene Uredbe o koncentracijama. Međutim konačna odluka još nije donesena.

⁽¹⁾ SL L 24, 29.1.2004., str. 1. („Uredba o koncentracijama”).

U skladu s Obavijesti Komisije o pojednostavnjenom postupku za postupanje s određenim koncentracijama prema Uredbi Vijeća (EZ) br. 139/2004 ⁽²⁾ treba napomenuti da je ovaj predmet primjeren za primjenu postupka iz Obavijesti.

5. Komisija poziva zainteresirane treće osobe da joj podnesu moguća očitovanja o predloženoj koncentraciji.

Očitovanja se Komisiji moraju dostaviti najkasnije u roku od 10 dana od datuma ove objave. U svakom je očitovanju potrebno navesti referentnu oznaku:

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

Očitovanja se Komisiji mogu poslati e-poštom ili poštom. Podaci za kontakt:

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

Poštanska adresa:

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

⁽²⁾ SL C 366, 14.12.2013., str. 5.

ISSN 1977-1088 (elektroničko izdanje)

ISSN 1977-060X (tiskano izdanje)



Ured za publikacije
Evropske unije
L-2985 Luxembourg
LUKSEMBURG

HR