ROZHODNUTIA

ROZHODNUTIE RADY (SZBP) 2019/797

zo 17. mája 2019,

o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty

RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o Európskej únii, a najmä jej článok 29,

so zreteľom na návrh vysokého predstaviteľa Únie pre zahraničné veci a bezpečnostnú politiku,

keďže:

(1) Rada 19. júna 2017 prijala závery o rámci pre spoločnú diplomatickú reakciu na škodlivé kybernetické činnosti (ďalej len „súbor nástrojov kybernetickej diplomacie"), v ktorých Rada vyjadrila obavy nad narastajúcou schopnosťou a odhodlaním štátnych a neštátnych subjektov presadzovať svoje ciele škodlivými kybernetickými činnosťami a potvrdila rastúcu potrebu chrániť integritu a bezpečnosť Únie, jej členských štátov a ich občanov pred kybernetickými hrozbami a škodlivými kybernetickými činnosťami.

(2) Rada zdôraznila, že jasná komunikácia pravdepodobných následkov spoločnej diplomatickej reakcie Únie na takéto škodlivé kybernetické činnosti má vplyv na správanie potenciálnych útočníkov v kybernetickom priestore, a tým sa ňou posilňuje bezpečnosť Únie a jej členských štátov. Takisto potvrdila, že opatrenia v rámci spoločnej zahraničnej a bezpečnostnej politiky (SZBP), v prípade potreby vrátane reštriktívnych opatrení, prijaté na základe príslušných ustanovení zmlúv sú vhodné pre rámec pre spoločnú diplomatickú reakciu Únie na škodlivé kybernetické činnosti s cieľom podporovať spoluprácu, uľahčovať zmierňovanie bezprostredných a dlhodobých hrozieb a ovplyvňovať správanie potenciálnych útočníkov v dlhodobom horizonte.

(3) Politický a bezpečnostný výbor prijal 11. októbra 2017 vykonávacie usmernenia k súboru nástrojov kybernetickej diplomacie. Vo vykonávacích usmerneniach sa uvádza päť kategórií opatrení v rámci súboru nástrojov kybernetickej diplomacie vrátane reštriktívnych opatrení, ako aj postup, ako tieto opatrenia odvolať.

(4) V záveroch Rady zo 16. apríla 2018 o škodlivých kybernetických činnostiach sa dôrazne odsúdilo škodlivé využívanie informačných a komunikačných technológií (IKT) a zdôraznilo sa, že využívanie IKT na škodlivé účely je neprijateľné, pretože sa tým oslabuje stabilita, bezpečnosť a prínosy, ktoré prináša internet a využívanie IKT. Rada pripomenula, že súborom nástrojov kybernetickej diplomacie sa prispieva k predchádzaniu konfliktom, spolupráci a stabilite v kybernetickom priestore tým, že sa ním v rámci SZBP stanovili opatrenia vrátane reštriktívnych opatrení, ktoré možno použiť pri predchádzaní škodlivým kybernetickým činnostiam a reakcii na ne. Uviedla, že Únia bude naďalej dôrazne presadzovať existujúce medzinárodné právo, ktoré sa vzťahuje na kybernetický priestor, a zdôraznila, že dodržiavanie medzinárodného práva, najmä Charty Organizácie Spojených národov, je základným predpokladom zachovania mieru a stability. Rada tiež zdôraznila, že štáty na páchanie medzinárodného protiprávneho konania informačnými a komunikačnými technológiami nesmú používať zástupné subjekty a mali by sa usilovať zabezpečiť, aby ich územie nevyužívali neštátne subjekty na páchanie takýchto aktov, ako sa uvádza v správe skupiny vládnych expertov OSN pre vývoj v oblasti informatiky a telekomunikácií v kontexte medzinárodnej bezpečnosti za rok 2015.

(5) Európska rada 28. júna 2018 prijala závery, v ktorých zdôraznila, že je potrebné posilniť spôsobilosti na boj proti hrozbám v oblasti kybernetickej bezpečnosti, ktoré majú pôvod mimo Únie. Európska rada požiadala inštitúcie a členské štáty, aby vykonali opatrenia uvedené v spoločnom oznámení Komisie a vysokého predstaviteľa Únie pre zahraničné veci a bezpečnostnú politiku z 13. júna 2018 s názvom „Zvyšovanie odolnosti a posilňovanie spôsobilosti riešiť hybridné hrozby" vrátane praktického využívania súboru nástrojov kybernetickej diplomacie.

(6) Európska rada 18. októbra 2018 prijala závery, v ktorých vyzvala, aby sa v nadväznosti na závery Rady z 19. júna 2017 pokročilo v práci zameranej na schopnosť reagovať na kybernetické útoky a odrádzať od nich prostredníctvom reštriktívnych opatrení Únie.

(7) V tejto súvislosti sa v tomto rozhodnutí stanovuje rámec cielených reštriktívnych opatrení na odrádzanie od kybernetických útokov so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty, a na reakciu na ne. Keď sa to považuje za potrebné na dosiahnutie cieľov SZBP v príslušných ustanoveniach článku 21 Zmluvy o Európskej únii, toto rozhodnutie umožňuje, aby sa reštriktívne opatrenia uplatnili aj v reakcii na kybernetické útoky so závažným vplyvom na tretie štáty alebo medzinárodné organizácie.

(8) Aby cielené reštriktívne opatrenia mali odstrašujúci a odradzujúci účinok, mali by sa zamerať na kybernetické útoky, ktoré patria do rozsahu pôsobnosti tohto rozhodnutia a ktoré sa vykonali úmyselne.

(9) Cielené reštriktívne opatrenia by sa mali rozlišovať od pripísania zodpovednosti za kybernetické útoky tretiemu štátu. Uplatňovanie cielených reštriktívnych opatrení nepredstavuje takéto pripísanie zodpovednosti, ktoré je zvrchovaným politickým rozhodnutím, ktoré sa prijíma v jednotlivých prípadoch. Každý členský štát má možnosť prijať vlastné rozhodnutie o priznaní zodpovednosti za kybernetické útoky tretiemu štátu.

(10) Na vykonanie niektorých opatrení je potrebná ďalšia činnosť Únie,

PRIJALA TOTO ROZHODNUTIE:

Článok 1

1. Toto rozhodnutie sa vzťahuje na kybernetické útoky so závažným vplyvom vrátane pokusov o kybernetické útoky s potenciálne závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty.

2. Kybernetické útoky, ktoré predstavujú vonkajšiu hrozbu, sú útoky, ktoré:

a) majú pôvod alebo sú vykonané mimo Únie;

b) využívajú infraštruktúru mimo Únie;

c) vykonáva fyzická alebo právnická osoba, subjekt alebo orgán, ktorý je usadený alebo je činný mimo Únie; alebo

d) sa uskutočňujú s podporou, pod vedením alebo kontrolou akejkoľvek fyzickej alebo právnickej osoby, subjektu alebo orgánu, ktorý je činný mimo Únie.

3. Na tento účel sú kybernetickými útokmi činnosti, ktoré zahŕňajú niektoré z týchto prvkov:

a) prístup do informačných systémov;

b) zásah do informačného systému;

c) zásah do údajov alebo

d) zachytávanie údajov,

ak nie sú takéto činnosti náležite povolené vlastníkom systému alebo údajov alebo ich časti alebo iným držiteľom práv k nim, alebo nie sú povolené podľa práva Únie alebo práva dotknutého členského štátu.

4. Kybernetické útoky, ktoré predstavujú hrozbu pre členské štáty, zahŕňajú útoky na informačné systémy týkajúce sa okrem iného:

a) kritickej infraštruktúry vrátane podmorských káblov a predmetov vypustených do kozmického priestoru, ktoré sú nevyhnutné na zachovanie základných funkcií spoločnosti alebo zdravia, ochrany, bezpečnosti a kvality života obyvateľov z ekonomického alebo sociálneho hľadiska;

b) služieb nevyhnutných na zachovanie základných spoločenských a/alebo hospodárskych činností, najmä v oblasti energetiky (elektrina, ropa a plyn); dopravy (vzdušnej, železničnej, vodnej a cestnej); bankovníctva; infraštruktúry finančných trhov; zdravotníctva (poskytovateľov zdravotnej starostlivosti, nemocníc a súkromných kliník); dodávky a distribúcie pitnej vody; digitálnej infraštruktúry a akéhokoľvek iného odvetvia, ktoré je pre dotknutý členský štát nevyhnutné;

c) kritických funkcií štátu, najmä v oblasti obrany, riadenia a fungovania inštitúcií vrátane volieb do verejných funkcií alebo hlasovania, fungovania hospodárskej a občianskej infraštruktúry, vnútornej bezpečnosti a zahraničných vzťahov, a to aj prostredníctvom diplomatických misií;

d) uchovávania utajovaných skutočností alebo manipulovania s nimi, alebo

e) tímov reakcie na núdzové situácie, ktoré sú súčasťou verejnej správy.

5. Kybernetické útoky, ktoré predstavujú hrozbu pre Úniu, zahŕňajú útoky zamerané na jej inštitúcie, orgány, úrady a agentúry, na jej delegácie v tretích krajinách alebo pri medzinárodných organizáciách, na jej operácie a misie spoločnej bezpečnostnej a obrannej politiky (SBOP) a na jej osobitných zástupcov.

6. Keď sa to považuje za potrebné na dosiahnutie cieľov SZBP v príslušných ustanoveniach článku 21 Zmluvy o Európskej únii, môžu sa reštriktívne opatrenia podľa tohto rozhodnutia uplatniť aj v reakcii na kybernetické útoky so závažným vplyvom na tretie štáty alebo medzinárodné organizácie.

Článok 2

Na účely tohto rozhodnutia sa uplatňujú tieto vymedzenia pojmov:

a) „informačný systém“ je zariadenie alebo skupina navzájom prepojených alebo súvisiacich zariadení, z ktorých jedno alebo viaceré automaticky spracúvajú digitálne údaje podľa programu, ako aj digitálne údaje, ktoré toto zariadenie alebo skupina zariadení ukladá, spracúva, opätovne získava alebo prenáša na účely svojho fungovania, používania, ochrany a údržby;

b) „zásah do informačného systému“ je bránenie fungovaniu informačného systému alebo prerušenie jeho fungovania vložením digitálnych údajov, prenosom, poškodením, vymazaním, zhoršením, pozmenením alebo potlačením takýchto údajov alebo ich zneprístupnením;

c) „zásah do údajov“ je vymazanie, poškodenie, zhoršenie, pozmenenie alebo potlačenie digitálnych údajov v informačnom systéme alebo zneprístupnenie takýchto údajov. Zahŕňa aj krádež údajov, finančných prostriedkov, hospodárskych zdrojov alebo duševného vlastníctva;

d) „zachytávanie údajov“ je zachytávanie údajov prostredníctvom technických prostriedkov, neverejného prenosu digitálnych údajov do informačného systému, z informačného systému alebo v rámci neho vrátane elektromagnetického vysielania z informačného systému nesúceho takéto digitálne údaje.

Článok 3

Faktory, podľa ktorých sa určuje, či má kybernetický útok závažný vplyv uvedený v článku 1 ods. 1, zahŕňajú okrem iného:

a) rozsah, mieru, dosah alebo závažnosť spôsobeného narušenia, a to aj pokiaľ ide o hospodárske a spoločenské činnosti, základné služby, kritické funkcie štátu, verejný poriadok alebo verejnú bezpečnosť;

b) počet dotknutých fyzických alebo právnických osôb, subjektov alebo orgánov;

c) počet dotknutých členských štátov;

d) výšku spôsobenej hospodárskej straty, napríklad rozsiahlou krádežou finančných prostriedkov, hospodárskych zdrojov alebo duševného vlastníctva;

e) majetkový prospech, ktorý páchateľ získal pre seba alebo iné osoby;

f) množstvo alebo povahu odcudzených údajov alebo rozsah porušenia ochrany údajov; alebo

g) povahu citlivých obchodných údajov, ku ktorým sa získal prístup.

Článok 4

1. Členské štáty prijmú opatrenia potrebné na zabránenie vstupu na svoje územia alebo prechodu cez svoje územia:

a) fyzickým osobám, ktoré sú zodpovedné za kybernetické útoky alebo pokusy o kybernetické útoky;

b) fyzickým osobám, ktoré poskytujú finančnú, technickú alebo materiálnu podporu na účely kybernetických útokov alebo sa inak podieľajú na kybernetických útokoch alebo pokusoch o kybernetické útoky, a to aj prostredníctvom plánovania, prípravy, účasti, riadenia, pomoci alebo podnecovania na takéto útoky alebo ich uľahčovania konaním alebo opomenutím;

c) fyzickým osobám, ktoré sú spojené s osobami, na ktoré sa vzťahujú písmená a) a b);

ktoré sú uvedené na zozname v prílohe.

2. Odsekom 1 sa členskému štátu neukladá povinnosť odmietnuť vstup svojim vlastným štátnym príslušníkom na svoje územie.

3. Odsekom 1 nie sú dotknuté prípady, v ktorých je členský štát viazaný záväzkom medzinárodného práva, a to:

a) ako hostiteľská krajina medzinárodnej medzivládnej organizácie;

b) ako hostiteľská krajina medzinárodnej konferencie zvolanej Organizáciou Spojených národov alebo zvolanej pod jej záštitou;

c) podľa mnohostrannej dohody, ktorou sa priznávajú výsady a imunity, alebo

d) na základe Zmluvy o zmierení z roku 1929 (Lateránska dohoda), ktorú uzavrela Svätá stolica (Vatikánsky mestský štát) a Taliansko.

4. Odsek 3 sa považuje za uplatniteľný aj v prípadoch, keď je členský štát hostiteľskou krajinou Organizácie pre bezpečnosť a spoluprácu v Európe (OBSE).

5. Rade sa náležite oznámia všetky prípady, v ktorých členský štát udelí výnimku podľa odseku 3 alebo 4.

6. Členské štáty môžu udeliť výnimky z opatrení uložených podľa odseku 1, ak je vycestovanie odôvodnené naliehavou humanitárnou potrebou alebo účasťou na medzivládnych zasadnutiach alebo na zasadnutiach, ktoré podporuje alebo organizuje Únia alebo ktoré organizuje členský štát predsedajúci OBSE a na ktorých sa vedie politický dialóg, ktorým sa priamo podporujú politické ciele reštriktívnych opatrení vrátane bezpečnosti a stability v kybernetickom priestore.

7. Členské štáty môžu tiež udeliť výnimky z opatrení uložených podľa odseku 1, ak je vstup alebo prechod potrebný na účely súdneho konania.

8. Členský štát, ktorý si želá udeliť výnimky uvedené v odseku 6 alebo 7, to písomne oznámi Rade. Výnimka sa považuje za udelenú, ak jeden alebo viacerí členovia Rady nevznesú písomne námietku do dvoch pracovných dní od prijatia oznámenia o navrhovanej výnimke. V prípade, že jeden alebo viacerí členovia Rady vznesú námietku, môže Rada kvalifikovanou väčšinou rozhodnúť o udelení navrhovanej výnimky.

9. Ak členský štát podľa odsekov 3, 4, 6, 7 alebo 8 povolí osobám uvedeným na zozname v prílohe vstup na svoje územie alebo prechod cezeň, toto povolenie sa prísne obmedzí na účel, na ktorý bolo udelené, a na osoby, ktorých sa priamo týka.

Článok 5

1. Zmrazujú sa všetky finančné prostriedky a hospodárske zdroje, ktoré patria:

a) fyzickým alebo právnickým osobám, subjektom alebo orgánom, ktoré sú zodpovedné za kybernetické útoky alebo pokusy o kybernetické útoky;

b) fyzickým alebo právnickým osobám, subjektom alebo orgánom, ktoré poskytujú finančnú, technickú alebo materiálnu podporu na účely kybernetických útokov alebo sa na kybernetických útokoch alebo na pokusoch o kybernetické útoky inak podieľajú, a to aj prostredníctvom plánovania, prípravy, účasti, riadenia, pomoci alebo podnecovania na takéto útoky alebo ich uľahčovania konaním alebo opomenutím;

c) fyzickým alebo právnickým osobám, subjektom alebo orgánom spojeným s fyzickými alebo právnickými osobami, subjektmi alebo orgánmi uvedenými v písmenách a) a b),

uvedeným na zozname v prílohe, alebo sú v ich vlastníctve, držbe alebo pod ich kontrolou.

2. Fyzickým alebo právnickým osobám, subjektom alebo orgánom uvedeným na zozname v prílohe sa priamo ani nepriamo, a ani v ich prospech nesprístupnia žiadne finančné prostriedky ani hospodárske zdroje.

3. Odchylne od odsekov 1 a 2 môžu príslušné orgány členských štátov povoliť uvoľnenie určitých zmrazených finančných prostriedkov alebo hospodárskych zdrojov alebo sprístupnenie určitých finančných prostriedkov alebo hospodárskych zdrojov za podmienok, ktoré považujú za vhodné, po tom, ako rozhodnú, že dané finančné prostriedky alebo hospodárske zdroje sú:

a) nevyhnutné na uspokojenie základných potrieb fyzických osôb uvedených na zozname v prílohe a ich nezaopatrených rodinných príslušníkov vrátane platieb za potraviny, nájom alebo hypotéku, lieky a lekárske ošetrenie, úhradu daní, poistného a poplatkov za verejnoprospešné služby;

b) určené výlučne na úhradu primeraných honorárov a náhradu výdavkov, ktoré vznikli v súvislosti s poskytovaním právnych služieb;

c) určené výlučne na úhradu poplatkov alebo nákladov na služby spojené s bežným vedením alebo správou zmrazených finančných prostriedkov alebo hospodárskych zdrojov;

d) potrebné na mimoriadne výdavky pod podmienkou, že relevantný príslušný orgán oznámil príslušným orgánom ostatných členských štátov a Komisii najmenej dva týždne pred udelením povolenia dôvody, na základe ktorých sa domnieva, že by sa osobitné povolenie malo udeliť; alebo

e) určené na úhradu na účet alebo z účtu diplomatickej misie alebo konzulárneho úradu či medzinárodnej organizácie, ktoré v súlade s medzinárodným právom požívajú imunity, pokiaľ sa takéto platby majú použiť na oficiálne účely diplomatickej misie alebo konzulárneho úradu či medzinárodnej organizácie.

Dotknutý členský štát informuje ostatné členské štáty a Komisiu o každom povolení udelenom podľa tohto odseku.

4. Odchylne od odseku 1 môžu príslušné orgány členských štátov povoliť uvoľnenie určitých zmrazených finančných prostriedkov alebo hospodárskych zdrojov, ak sú splnené tieto podmienky:

a) na finančné prostriedky alebo hospodárske zdroje sa vzťahuje arbitrážne rozhodnutie, ktoré bolo vydané pred dátumom zaradenia fyzickej alebo právnickej osoby, subjektu alebo orgánu uvedených v odseku 1 na zoznam v prílohe, alebo sa na ne vzťahuje súdne či správne rozhodnutie vydané v Únii, alebo súdne rozhodnutie vykonateľné v dotknutom členskom štáte pred uvedeným dátumom alebo po ňom;

b) finančné prostriedky alebo hospodárske zdroje sa použijú výlučne na uspokojenie pohľadávok zabezpečených takýmto rozhodnutím alebo uznaných za platné v takomto rozhodnutí, a to v rámci obmedzení stanovených uplatniteľnými zákonmi a inými právnymi predpismi, ktorými sa riadia práva osôb s takýmito pohľadávkami;

c) rozhodnutie nie je v prospech fyzickej alebo právnickej osoby, subjektu alebo orgánu, ktoré sú uvedené na zozname v prílohe, a

d) uznanie rozhodnutia nie je v rozpore s verejným poriadkom v dotknutom členskom štáte.

Dotknutý členský štát informuje ostatné členské štáty a Komisiu o každom povolení udelenom podľa tohto odseku.

5. Odsek 1 nebráni tomu, aby fyzická alebo právnická osoba, subjekt alebo orgán uvedené na zozname v prílohe vykonali platbu splatnú na základe zmluvy, ktorá sa uzavrela pred dátumom, keď boli takáto fyzická alebo právnická osoba, subjekt alebo orgán zaradené na zoznam, pod podmienkou, že dotknutý členský štát dospel k záveru, že príjemcom platby nie je priamo ani nepriamo fyzická alebo právnická osoba, subjekt alebo orgán uvedené v odseku 1.

6. Odsek 2 sa neuplatňuje, keď sa na zmrazené účty pripisujú:

a) úroky alebo iné výnosy z týchto účtov;

b) platby splatné na základe zmlúv, dohôd alebo záväzkov, ktoré sa uzavreli alebo ktoré vznikli pred dátumom, od ktorého tieto účty začali podliehať opatreniam stanoveným v odsekoch 1 a 2; alebo

c) platby splatné na základe súdneho, správneho alebo arbitrážneho rozhodnutia vydaného v Únii alebo vykonateľného v dotknutom členskom štáte;

pod podmienkou, že sa na všetky takéto úroky, iné výnosy a platby naďalej vzťahujú opatrenia stanovené v odseku 1.

Článok 6

1. Rada konajúc jednomyseľne na návrh členského štátu alebo vysokého predstaviteľa Únie pre zahraničné veci a bezpečnostnú politiku zostavuje zoznam uvedený v prílohe a vykonáva v ňom zmeny.

2. Rada oznámi rozhodnutia uvedené v odseku 1 vrátane dôvodov zaradenia na zoznam dotknutej fyzickej alebo právnickej osobe, subjektu alebo orgánu buď priamo, ak je ich adresa známa, alebo prostredníctvom uverejnenia oznámenia, a poskytne tak uvedenej fyzickej alebo právnickej osobe, subjektu alebo orgánu možnosť vyjadriť pripomienky.

3. Ak sa predložia pripomienky alebo zásadné nové dôkazy, Rada preskúma rozhodnutia uvedené v odseku 1 a dotknutú fyzickú alebo právnickú osobu, subjekt alebo orgán o tom zodpovedajúcim spôsobom informuje.

Článok 7

1. V prílohe sa uvádzajú dôvody zaradenia fyzických a právnických osôb, subjektov a orgánov podľa článkov 4 a 5 na zoznam.

2. V prílohe sa uvádzajú informácie potrebné na identifikáciu dotknutých fyzických alebo právnických osôb, subjektov alebo orgánov, ak sú dostupné. V prípade fyzických osôb môžu tieto informácie zahŕňať mená a prezývky, dátum a miesto narodenia, štátnu príslušnosť, číslo cestovného pasu a preukazu totožnosti, pohlavie, adresu, ak je známa, a funkciu alebo povolanie. V prípade právnických osôb, subjektov alebo orgánov môžu tieto informácie zahŕňať názvy, miesto a dátum registrácie, registračné číslo a miesto podnikania.

Článok 8

Neuznajú sa žiadne nároky v súvislosti so žiadnou zmluvou alebo transakciou, ktorých plnenie bolo priamo alebo nepriamo, úplne alebo čiastočne, dotknuté opatreniami uloženými podľa tohto rozhodnutia, vrátane nárokov na náhradu škody alebo akýchkoľvek iných nárokov tohto druhu, ako je napríklad nárok na kompenzáciu alebo pohľadávka so zárukou, predovšetkým nárok na predĺženie platnosti alebo vyplatenie dlhopisu, záruky alebo sľubu odškodnenia, najmä finančnej záruky alebo finančného zabezpečenia v akejkoľvek forme, ak ich predložia:

a) označené fyzické alebo právnické osoby, subjekty alebo orgány uvedené na zozname v prílohe;

b) akákoľvek fyzická alebo právnická osoba, subjekt alebo orgán konajúce prostredníctvom alebo v mene niektorej z fyzických alebo právnických osôb, subjektov alebo orgánov uvedených v písmene a).

Článok 9

Na dosiahnutie čo najväčšieho účinku opatrení ustanovených v tomto rozhodnutí Únia vyzýva tretie štáty, aby prijali reštriktívne opatrenia podobné tým, ktoré sa stanovujú v tomto rozhodnutí.

Článok 10

Toto rozhodnutie sa uplatňuje do 18. mája 2020 a pravidelne sa preskúmava. Podľa potreby sa predĺži jeho účinnosť alebo bude zmenené, ak Rada usúdi, že sa jeho ciele nedosiahli.

Článok 11

Toto rozhodnutie nadobúda účinnosť dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie*.

V Bruseli 17. mája 2019

Za Radu

predseda

E.O. TEODOROVICI

PRÍLOHA

Zoznam fyzických a právnických osôb, subjektov a orgánov podľa článkov 4 a 5

[…]