Rada
Unii Europejskiej

Bruksela, 14 maja 2019 r.
(OR. en)

7299/19

LIMITE

CORLX 106
CFSP/PESC 191
RELEX 235
CYBER 81
JAI 264
FIN 216

AKTY USTAWODAWCZE I INNE INSTRUMENTY

Dotyczy:	DECYZJA RADY w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim

DECYZJA RADY (WPZiB) 2019/...

z dnia ...

w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 29,

uwzględniając wniosek Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa,

a także mając na uwadze, co następuje:

(1) 19 czerwca 2017 r. Rada przyjęła konkluzje dotyczące ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne (zwanych dalej „zestawem narzędzi dla dyplomacji cyfrowej”), w których Rada wyraziła zaniepokojenie rosnącą zdolnością i gotowością podmiotów państwowych i niepaństwowych do realizowania swoich celów za pomocą szkodliwych działań w cyberprzestrzeni i podkreśliła rosnącą potrzebę chronienia integralności i bezpieczeństwa Unii, jej państw członkowskich oraz ich obywateli przed zagrożeniami dla cyberbezpieczeństwa i szkodliwymi działaniami w cyberprzestrzeni.

(2) Rada podkreśliła, że wyraźne sygnalizowanie prawdopodobnych konsekwencji, jakie nastąpią w wyniku wspólnej unijnej reakcji dyplomatycznej na takie szkodliwe działania w cyberprzestrzeni, wpływa na zachowania potencjalnych agresorów w tej przestrzeni i tym samym wzmacnia bezpieczeństwo Unii i jej państw członkowskich. Rada potwierdziła też, że środki przewidziane w ramach wspólnej polityki zagranicznej i bezpieczeństwa (WPZiB), w tym w razie konieczności środki ograniczające przyjmowane zgodnie z odpowiednimi postanowieniami traktatów stanowią odpowiednie ramy wspólnej reakcji dyplomatycznej na szkodliwe działania w cyberprzestrzeni i mają zachęcać do współpracy, ułatwiać ograniczanie bezpośrednich i długoterminowych zagrożeń oraz w perspektywie długoterminowej wpływać na zachowania potencjalnych agresorów.

(3) W dniu 11 października 2017 r. Komitet Polityczny i Bezpieczeństwa zatwierdził wytyczne wykonawcze dotyczące zestawu narzędzi dla dyplomacji cyfrowej. Wytyczne te odnoszą się do pięciu kategorii środków, w tym środków ograniczających, w ramach zestawu narzędzi dla dyplomacji cyfrowej, a także do procesu stosowania tych środków.

(4) W konkluzjach Rady z dnia 16 kwietnia 2018 r. w sprawie szkodliwych działań w cyberprzestrzeni stanowczo potępiono szkodliwe użycie technologii informacyjno-komunikacyjnej (ICT) i podkreślono, że użycie ICT do szkodliwych celów jest nie do zaakceptowania, ponieważ podważa stabilność, bezpieczeństwo i korzyści, jakie zapewnia internet i używanie ICT. Rada przypomniała, że zestaw narzędzi dla dyplomacji cyfrowej przyczynia się do zapobiegania konfliktom, do współpracy i stabilności w cyberprzestrzeni przez określanie środków w ramach WPZiB, w tym środków ograniczających, które mogą być stosowane do zapobiegania szkodliwym działaniom w cyberprzestrzeni i reagowania na nie. Stwierdziła, że Unia będzie nadal zdecydowanie stać na straży tego, aby istniejące prawo międzynarodowe miało zastosowanie do cyberprzestrzeni, oraz podkreśliła, że poszanowanie prawa międzynarodowego, w szczególności Karty Narodów Zjednoczonych, ma podstawowe znaczenie dla utrzymania pokoju i stabilności. Rada podkreśliła również, że państwa mają nie używać serwerów proxy do popełniania czynów, które są niezgodne z prawem międzynarodowym, przy stosowaniu ICT i że państwa powinny dążyć do zapewnienia, aby ich terytorium nie było wykorzystywane przez podmioty niepaństwowe do popełniania takich czynów, zgodnie z treścią sprawozdania z 2015 r. sporządzonego przez ONZ-owskie grupy ekspertów rządowych dotyczące rozwoju w dziedzinie informacji i telekomunikacji w kontekście bezpieczeństwa międzynarodowego.

(5) 28 czerwca 2018 r. Rada Europejska przyjęła konkluzje, w których pokreślono potrzebę wzmocnienia zdolności w zakresie eliminowania zagrożeń dla cyberbezpieczeństwa pochodzących spoza Unii. Rada Europejska wezwała instytucje i państwa członkowskie do wdrożenia środków, o których mowa we wspólnym komunikacie Komisji i Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa z dnia 13 września 2017 r. zatytułowanym „Zwiększenie odporności i wzmocnienie zdolności reagowania na zagrożenia hybrydowe", w tym do praktycznego zastosowania zestawu narzędzi dla dyplomacji cyfrowej.

(6) 18 października 2018 r. Rada Europejska przyjęła konkluzje, w których wezwała do kontynuowania prac nad zdolnościami do reagowania na cyberataki i zapobiegania im z wykorzystaniem unijnych środków ograniczających – zgodnie z konkluzjami Rady z 19 czerwca 2017 r.

(7) W tym kontekście niniejsza decyzja ustanawia ramy dla ukierunkowanych środków ograniczających służących zapobieganiu cyberatakom i reagowaniu na cyberataki, które wywołują poważne skutki i stanowią zewnętrzne zagrożenie dla Unii lub jej państw członkowskich. Jeżeli uznaje się to za konieczne do osiągnięcia celów WPZiB określonych w odpowiednich postanowieniach art. 21 Traktatu o Unii Europejskiej, niniejsza decyzja pozwala również, aby środki ograniczające były stosowane w odpowiedzi na wywołujące poważne skutki cyberataki wymierzone przeciwko państwom trzecim lub organizacjom międzynarodowym.

(8) Z myślą o uzyskaniu efektów odstraszających i zniechęcających, ukierunkowane środki ograniczające powinny koncentrować się na wchodzących w zakres niniejszej decyzji cyberatakach, które są przeprowadzane celowo.

(9) Należy rozróżnić ukierunkowane środki ograniczające i ustalenie państwa trzeciego odpowiedzialnego za cyberataki. Zastosowanie takich ukierunkowanych środków ograniczających nie jest równoznaczne z takim ustaleniem, które stanowi suwerenną decyzję polityczną podejmowaną w trybie indywidualnym. Każde państwo członkowskie ma swobodę w dokonaniu ustalenia, które państwo trzecie jest odpowiedzialne za cyberataki.

(10) Unia musi podjąć dalsze działania, aby wprowadzić w życie niektóre środki,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

1. Niniejsza decyzja ma zastosowanie do cyberataków wywołujących poważne skutki – w tym do usiłowania przeprowadzenia cyberataków mogących wywoływać poważne skutki – które to ataki stanowią zewnętrzne zagrożenie dla Unii lub jej państw członkowskich.

2. Cyberataki stanowiące zewnętrzne zagrożenie obejmują cyberataki, które:

   a) zostały przygotowane poza terytorium Unii lub są przeprowadzane spoza terytorium Unii;

   b) wykorzystują infrastrukturę znajdującą się poza terytorium Unii;

   c) są przeprowadzane przez osobę fizyczną lub prawną, podmiot lub organ, które mają siedzibę lub prowadzą działalność poza terytorium Unii; lub

   d) są przeprowadzane przy wsparciu, na zlecenie lub pod kontrolą osoby fizycznej lub prawnej, podmiotu lub organu, które prowadzą działalność poza terytorium Unii.

3. W związku z powyższym cyberataki są działaniami obejmującymi co najmniej jeden z następujących elementów:

   a) dostęp do systemów informacyjnych;

   b) ingerencja w systemy informacyjne;

   c) ingerencja w dane; lub

   d) przechwytywanie danych,

i przy założeniu że działania takie nie są prowadzone na podstawie należytego upoważnienia wydanego przez właściciela lub inny podmiot mający prawa do systemu lub danych lub ich części lub nie są dozwolone na mocy prawa Unii lub danego państwa członkowskiego.

4. Cyberataki stanowiące zagrożenie dla państw członkowskich obejmują cyberataki na systemy informacyjne związane, między innymi, z:

a) infrastrukturą krytyczną – w tym podmorskie kable i obiekty wystrzelone w przestrzeń kosmiczną – która jest niezbędna do utrzymania podstawowych funkcji społecznych lub zdrowia, bezpieczeństwa, ochrony i dobrobytu materialnego lub społecznego ludności;

b) usługami niezbędnymi do utrzymania podstawowej działalności społecznej lub gospodarczej, w szczególności w sektorze energii (energii elektrycznej, ropy naftowej i gazu), transportu (lotniczego, kolejowego, wodnego i drogowego), bankowości, infrastruktury rynków finansowych, zdrowia (ośrodki opieki zdrowotnej, szpitale i prywatne kliniki), zaopatrzenia w wodę pitną i jej dystrybucji, infrastruktury cyfrowej, oraz w każdym innym sektorze, który ma podstawowe znaczenie dla danego państwa członkowskiego;

c) krytycznymi funkcjami państwa, w szczególności w obszarze obrony, zarządzania instytucjami i ich funkcjonowania, w tym wyborów państwowych lub procesu głosowania, funkcjonowania infrastruktury gospodarczej i cywilnej, bezpieczeństwa wewnętrznego i stosunków zewnętrznych, w tym za pośrednictwem misji dyplomatycznych;

d) przechowywaniem lub przetwarzaniem informacji niejawnych; lub

e) rządowymi zespołami reagowania kryzysowego.

5. Cyberataki stanowiące zagrożenie dla Unii obejmują cyberataki przeprowadzane przeciwko jej instytucjom, organom i jednostkom organizacyjnym, jej delegaturom w państwach trzecich lub w organizacjach międzynarodowych, jej operacjom i misjom w dziedzinie wspólnej polityki bezpieczeństwa i obrony (WPBiO) oraz jej specjalnym przedstawicielom.

6. Jeżeli uznaje się to za konieczne do osiągnięcia celów WPZiB określonych w odpowiednich postanowieniach art. 21 Traktatu o Unii Europejskiej, środki ograniczające na mocy niniejszej decyzji można również stosować w odpowiedzi na wywołujące poważne skutki cyberataki wymierzone przeciwko państwom trzecim lub organizacjom międzynarodowym.

Artykuł 2

Do celów niniejszej decyzji stosuje się następujące definicje:

a) „systemy informacyjne” oznaczają urządzenie lub grupę wzajemnie połączonych lub powiązanych ze sobą urządzeń, z których przynajmniej jedno, zgodnie z programem, dokonuje automatycznego przetwarzania danych cyfrowych, jak również danych cyfrowych przechowywanych, przetwarzanych, wyszukiwanych lub przekazywanych przez to urządzenie lub tę grupę urządzeń, w celach eksploatacji, użycia, ochrony lub utrzymania tego urządzenia lub tej grupy urządzeń;

b) „ingerencja w system informacyjny” oznacza utrudnienie lub przerwanie funkcjonowania systemu informacyjnego przez wprowadzenie danych cyfrowych, przekazanie takich danych, ich uszkodzenie, usunięcie, pogorszenie ich jakości, ich zmianę lub wyeliminowanie bądź przez uczynienie ich niedostępnymi;

c) „ingerencja w dane” oznacza usunięcie, uszkodzenie, pogorszenie jakości, zmianę lub wyeliminowanie danych cyfrowych w systemie informacyjnym, bądź uczynienie ich niedostępnymi; obejmuje ona również kradzież danych, środków finansowych, zasobów gospodarczych lub praw własności intelektualnej;

d) „przechwycenie danych” oznacza przechwycenie, za pomocą środków technicznych, niepublicznych przekazów danych cyfrowych do systemu informacyjnego, z systemu informacyjnego lub w ramach takiego systemu, w tym emisji elektromagnetycznych z systemu informacyjnego zawierających takie dane cyfrowe.

Artykuł 3

Czynniki określające, czy cyberatak ma poważne skutki, o których mowa w art. 1 ust. 1, obejmują co najmniej jeden z następujących elementów:

a) zakres, skalę, wpływ lub stopień spowodowanych zakłóceń m.in. działalności gospodarczej i społecznej, usług kluczowych, krytycznych funkcji państwa, porządku publicznego lub bezpieczeństwa publicznego;

b) liczbę osób fizycznych lub prawnych, podmiotów lub organów, których dotyczy cyberatak;

c) liczbę państw członkowskich, których dotyczy cyberatak;

d) wielkość poniesionych strat gospodarczych, na przykład w wyniku zakrojonej na szeroką skalę kradzieży środków finansowych, zasobów gospodarczych lub praw własności intelektualnej;

e) korzyść ekonomiczną odniesioną przez sprawcę dla siebie lub dla innych osób;

f) ilość lub charakter ukradzionych danych lub skalę naruszenia ochrony danych; lub

g) charakter poufnych danych handlowych, do których uzyskano dostęp.

Artykuł 4

1. Państwa członkowskie przyjmują środki niezbędne do uniemożliwienia wjazdu na ich terytoria lub tranzytu przez te terytoria:

   a) osób fizycznych odpowiedzialnych za przeprowadzenie lub usiłowanie przeprowadzenia cyberataków;

   b) osób fizycznych, które zapewniają finansowe, techniczne lub materialne wsparcie dla cyberataków lub usiłowania przeprowadzenia cyberataków, bądź też w inny sposób angażują się w takie ataki, w tym przez ich planowanie, przygotowywanie, uczestnictwo w nich, kierowanie nimi, pomoc w nich lub zachęcanie do takich ataków lub ułatwianie ich poprzez działanie lub zaniechanie;

   c) osób fizycznych powiązanych z osobami fizycznymi, o których mowa w lit. a) i b);

   których wykaz zamieszczono w załączniku.

2. Ust. 1 nie zobowiązuje państwa członkowskiego do odmowy jego własnym obywatelom wjazdu na jego terytorium.

3. Ust. 1 pozostaje bez uszczerbku dla przypadków, gdy dane państwo członkowskie związane jest zobowiązaniem wynikającym z prawa międzynarodowego, a mianowicie:

   a) jest państwem goszczącym międzynarodową organizację międzyrządową;

   b) jest państwem goszczącym międzynarodową konferencję zwołaną przez Organizację Narodów Zjednoczonych lub pod jej auspicjami;

   c) na mocy umowy wielostronnej przyznającej przywileje i immunitety; lub

   d) na podstawie Traktatu pojednawczego (Traktatu laterańskiego) z 1929 r. zawartego między Stolicą Apostolską (Państwem Watykańskim) a Włochami.

4. Ust. 3 uznaje się za mający zastosowanie również w przypadkach, gdy dane państwo członkowskie jest krajem goszczącym Organizację Bezpieczeństwa i Współpracy w Europie (OBWE).

5. Rada jest należycie informowana o wszystkich przypadkach przyznania przez państwo członkowskie wyłączenia na mocy ust. 3 lub 4.

6. Państwa członkowskie mogą przyznawać wyłączenia ze środków nałożonych na podstawie ust. 1 w przypadkach, gdy podróż jest uzasadniona pilną potrzebą humanitarną lub uczestnictwem w posiedzeniach międzyrządowych lub posiedzeniach popieranych przez Unię lub których gospodarzem jest Unia lub dane państwo członkowskie sprawujące przewodnictwo w OBWE, gdzie prowadzony jest dialog polityczny bezpośrednio propagujący polityczne cele środków ograniczających, w tym zapewnienie bezpieczeństwa i stabilności cyberprzestrzeni.

7. Państwa członkowskie mogą też przyznawać wyłączenia ze środków nałożonych na podstawie ust. 1 w przypadkach, gdy wjazd lub przejazd jest konieczny w związku z uczestnictwem w postępowaniu sądowym.

8. Państwo członkowskie, które zamierza przyznać wyłączenia określone w ust. 6 lub 7, powiadamia o tym Radę na piśmie. Wyłączenie uważa się za przyznane, chyba że co najmniej jeden członek Rady wniesie sprzeciw na piśmie w ciągu dwóch dni roboczych od otrzymania powiadomienia o proponowanym wyłączeniu. W przypadku gdy co najmniej jeden członek Rady wniesie sprzeciw, Rada może postanowić o przyznaniu proponowanego wyłączenia, stanowiąc większością kwalifikowaną.

9. W przypadkach gdy zgodnie z ust. 3, 4, 6, 7 lub 8 państwo członkowskie zezwala na wjazd lub przejazd przez swoje terytorium osobom wymienionym w załączniku, zezwolenie jest ściśle ograniczone do celu, dla którego zostało wydane oraz do wymienionych w nim osób.

Artykuł 5

1. Wszelkie środki finansowe i zasoby gospodarcze należące do lub będące własnością, w posiadaniu lub znajdujące się pod kontrolą:

   a) osób fizycznych lub prawnych, podmiotów lub organów odpowiedzialnych za przeprowadzenie lub próby przeprowadzenia cyberataków;

   b) osób fizycznych lub prawnych, podmiotów lub organów, które zapewniają finansowe, techniczne lub materialne wsparcie dla cyberataków lub w celu usiłowania przeprowadzenia cyberataków, bądź też w inny sposób angażują się w takie ataki, w tym przez ich planowanie, przygotowywanie, uczestnictwo w nich, kierowanie nimi, pomoc w nich lub zachęcanie do takich ataków lub ułatwianie ich poprzez działanie lub zaniechanie;

   c) osób fizycznych lub prawnych, podmiotów lub organów powiązanych z osobami fizycznymi lub prawnymi, podmiotami lub organami, o których mowa w lit. a) i b) niniejszego ustępu;

   których wykaz zamieszczono w załączniku, zostają zamrożone.

2. Nie udostępnia się – bezpośrednio lub pośrednio – osobom fizycznym lub prawnym, podmiotom lub organom wymienionym w załączniku ani na ich rzecz żadnych środków finansowych ani zasobów gospodarczych.

3. W drodze odstępstwa od ust. 1 i 2 właściwe organy państwa członkowskiego mogą zezwolić na odblokowanie niektórych zamrożonych środków finansowych lub zasobów gospodarczych lub na udostępnienie ich na warunkach, jakie uznają za stosowne, po ustaleniu, że odnośne środki finansowe lub zasoby gospodarcze:

a) są niezbędne do zaspokojenia podstawowych potrzeb osób fizycznych wymienionych w załączniku oraz członków rodzin pozostających na utrzymaniu takich osób fizycznych, w tym opłat za żywność, z tytułu najmu lub kredytu hipotecznego, za leki i leczenie, z tytułu podatków, składek ubezpieczeniowych oraz opłat za usługi użyteczności publicznej;

b) są przeznaczone wyłącznie na pokrycie uzasadnionych kosztów honorariów lub zwrotów poniesionych wydatków związanych z usługami prawniczymi;

c) są przeznaczone wyłącznie na pokrycie opłat lub należności za usługi polegające na zwykłym przechowywaniu lub utrzymywaniu zamrożonych środków finansowych lub zasobów gospodarczych;

d) są niezbędne do pokrycia nadzwyczajnych wydatków, pod warunkiem że właściwy organ powiadomił właściwe organy pozostałych państw członkowskich oraz Komisję o powodach, dla których uważa, że należy udzielić szczególnego zezwolenia, co najmniej dwa tygodnie przed jego udzieleniem; lub

e) zostaną wpłacone na rachunek lub wypłacone z rachunku misji dyplomatycznej lub misji konsularnej lub organizacji międzynarodowej posiadającej immunitet na mocy prawa międzynarodowego, w zakresie, jakim płatności te są przeznaczone na oficjalne cele tej misji dyplomatycznej lub misji konsularnej lub organizacji międzynarodowej.

Dane państwo członkowskie informuje pozostałe państwa członkowskie oraz Komisję o wszelkich zezwoleniach udzielonych na podstawie niniejszego ustępu.

4. W drodze odstępstwa od ust. 1 właściwe organy państw członkowskich mogą zezwolić na odblokowanie niektórych zamrożonych środków finansowych lub zasobów gospodarczych, jeżeli spełnione są następujące warunki:

a) środki finansowe lub zasoby gospodarcze są przedmiotem orzeczenia arbitrażowego wydanego przed datą umieszczenia w wykazie znajdującym się w załączniku osoby fizycznej lub prawnej, podmiotu lub organu, o których mowa w ust. 1, lub orzeczenia sądowego lub decyzji administracyjnej wydanych w Unii, lub orzeczenia sądowego podlegającego wykonaniu w danym państwie członkowskim, przed tą datą lub po tej dacie;

b) środki finansowe lub zasoby gospodarcze zostaną wykorzystane wyłącznie w celu zaspokojenia roszczeń zabezpieczonych takim orzeczeniem lub decyzją lub uznanych za zasadne w takim orzeczeniu lub decyzji, w granicach określonych przez mające zastosowanie przepisy ustawowe i wykonawcze regulujące prawa osób, którym takie roszczenia przysługują;

c) orzeczenie lub decyzja nie przynoszą korzyści osobie fizycznej lub prawnej, podmiotowi lub organowi wymienionym w załączniku; oraz

d) uznanie tego orzeczenia lub tej decyzji nie jest sprzeczne z porządkiem publicznym danego państwa członkowskiego.

Dane państwo członkowskie informuje pozostałe państwa członkowskie oraz Komisję o wszelkich zezwoleniach udzielonych na podstawie niniejszego ustępu.

5. Ust. 1 nie uniemożliwia osobie fizycznej lub prawnej, podmiotowi lub organowi, wymienionym w załączniku, dokonywania płatności należnej z tytułu umowy zawartej przed dniem umieszczenia tej osoby fizycznej lub prawnej, takiego podmiotu lub takiego organu w wykazie znajdującym się w załączniku, pod warunkiem że dane państwo członkowskie ustaliło, że płatność nie jest bezpośrednio lub pośrednio dokonywana na rzecz osoby fizycznej lub prawnej, podmiotu lub organu, o których mowa w ust. 1.

6. Ust. 2 nie ma zastosowania do księgowania na zamrożonych rachunkach:

a) odsetek ani innych dochodów z tych rachunków;

b) płatności należnych z tytułu umów, porozumień lub zobowiązań, które zostały zawarte lub powstały przed datą objęcia tych rachunków środkami przewidzianymi w ust. 1 i 2; lub

c) płatności należnych z tytułu orzeczeń sądowych, decyzji administracyjnych lub orzeczeń arbitrażowych wydanych w Unii lub podlegających wykonaniu w danym państwie członkowskim,

pod warunkiem że wszelkie takie odsetki, inne dochody i płatności nadal podlegają środkom przewidzianym w ust. 1.

Artykuł 6

1. Rada, stanowiąc jednomyślnie na wniosek państwa członkowskiego lub Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa, sporządza i zmienia wykaz znajdujący się w załączniku.

2. Rada przekazuje decyzję, o której mowa w ust. 1, wraz z uzasadnieniem umieszczenia w wykazie, danej osobie fizycznej lub prawnej, danemu podmiotowi lub danemu organowi bezpośrednio – jeżeli adres jest znany – albo w drodze opublikowania ogłoszenia, umożliwiając takiej osobie fizycznej lub prawnej, takiemu podmiotowi lub takiemu organowi przedstawienie uwag.

3. W przypadku gdy zostaną zgłoszone uwagi lub przedstawione istotne nowe dowody, Rada dokonuje przeglądu decyzji, o której mowa w ust. 1, i informuje o tym daną osobę fizyczną lub prawną, dany podmiot lub dany organ.

Artykuł 7

1. Załącznik zawiera uzasadnienie umieszczenia w wykazie osób fizycznych i prawnych, podmiotów i organów, o których mowa w art. 4 i 5.

2. Załącznik zawiera – w przypadku gdy są one dostępne – informacje, które są niezbędne do zidentyfikowania danych osób fizycznych lub prawnych, podmiotów lub organów. W przypadku osób fizycznych informacje takie mogą obejmować imiona i nazwiska, w tym pseudonimy, datę i miejsce urodzenia, obywatelstwo, numery paszportu i dokumentu tożsamości, płeć, adres, jeśli jest znany, a także stanowisko lub zawód. W przypadku osób prawnych, podmiotów lub organów informacje takie mogą obejmować nazwy, miejsce i datę wpisu do rejestru, numer w rejestrze i miejsce prowadzenia działalności.

Artykuł 8

Nie są zaspokajane żadne roszczenia w związku z dowolną umową lub transakcją, których wykonanie zostało zakłócone, bezpośrednio lub pośrednio, w całości lub części, przez środki nałożone niniejszą decyzją, w tym roszczenia odszkodowawcze lub wszelkie inne roszczenia tego rodzaju, takie jak roszczenia o odszkodowanie lub roszczenia wynikające z gwarancji, w szczególności roszczenia o przedłużenie terminu płatności lub o zapłatę obligacji, gwarancji lub zabezpieczeń, w szczególności gwarancji finansowych lub finansowych listów gwarancyjnych, w dowolnej formie – o ile zostały one wniesione przez:

a) wskazane osoby fizyczne lub prawne, podmioty lub organy wymienione w wykazie w załączniku;

b) wszelkie osoby fizyczne lub prawne, podmioty lub organy działające za pośrednictwem lub w imieniu osób fizycznych lub prawnych, podmiotów lub organów, o których mowa w lit. a).

Artykuł 9

W celu maksymalizacji oddziaływania środków przewidzianych w niniejszej decyzji, Unia zachęca państwa trzecie do przyjmowania środków ograniczających podobnych do tych przewidzianych w niniejszej decyzji.

Artykuł 10

Niniejszą decyzję stosuje się do dnia ... [1 rok od daty wejścia w życie niniejszej decyzji]. Niniejsza decyzja jest poddawana stałemu przeglądowi. Jeżeli Rada uzna, że cele niniejszej decyzji nie zostały osiągnięte, jej okres obowiązywania zostanie przedłużony lub dokona się w niej odpowiednich zmian.

Artykuł 11

Niniejsza decyzja wchodzi w życie następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Sporządzono w ...

W imieniu Rady
Przewodniczący

ZAŁĄCZNIK

Wykaz osób fizycznych i prawnych, podmiotów i organów, o których mowa w art. 4 i 5

[…]