Czwartek, 13 marca 2014 r.

P7_TA(2014)0244

Wysoki poziom bezpieczeństwa sieci i informacji ***I

Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 13 marca 2014 r. w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii (COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

(Zwykła procedura ustawodawcza: pierwsze czytanie)

(2017/C 378/74)

Parlament Europejski,

— uwzględniając wniosek Komisji przedstawiony Parlamentowi i Radzie (COM(2013)0048),

— uwzględniając art. 294 ust. 2 oraz art. 114 Traktatu o funkcjonowaniu Unii Europejskiej, zgodnie z którymi wniosek został przedstawiony Parlamentowi przez Komisję (C7–0035/2013),

— uwzględniając art. 294 ust. 3 Traktatu o funkcjonowaniu Unii Europejskiej,

— uwzględniając uzasadnioną opinię przedstawioną przez Szwedzki Parlament na podstawie Protokołu nr 2 w sprawie stosowania zasad pomocniczości i proporcjonalności, zgodnie z którą projekt aktu ustawodawczego nie jest zgodny z zasadą pomocniczości,

— uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego z dnia 22 maja 2013 r. ([1]),

— uwzględniając swoją rezolucję z dnia 12 września 2013 r. w sprawie strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń ([2]),

— uwzględniając art.55 Regulaminu,

— uwzględniając sprawozdanie Komisji Rynku Wewnętrznego i Ochrony Konsumentów oraz opinie Komisji Przemysłu, Badań Naukowych i Energii, Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych oraz Komisji Spraw Zagranicznych (A7-0103/2014),

1. przyjmuje poniższe stanowisko w pierwszym czytaniu;

2. zwraca się do Komisji o ponowne przekazanie mu sprawy, jeśli uzna ona za stosowne wprowadzić znaczące zmiany do swojego wniosku lub zastąpić go innym tekstem;

3. zobowiązuje swojego przewodniczącego do przekazania stanowiska Parlamentu Radzie i Komisji, a także parlamentom narodowym.

P7_TC1-COD(2013)0027

Stanowisko Parlamentu Europejskiego przyjęte w pierwszym czytaniu w dniu 13 marca 2014 r. w celu przyjęcia dyrektywy Parlamentu Europejskiego i Rady 2014/…/UE w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 114,

---

([1]) Dz.U. C 271 z 19.9.2013, s. 133.
([2]) Teksty przyjęte, P7_TA(2013)0376.

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego ([1]),

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą ([2]),

a także mając na uwadze, co następuje:

(1) Sieci oraz systemy i usługi informatyczne pełnią w społeczeństwie istotną rolę. Ich niezawodność i bezpieczeństwo mają zasadnicze znaczenie dla ***wolności i ogólnego bezpieczeństwa obywateli Unii, a także dla*** działalności gospodarczej i dobrobytu społeczeństwa, a w szczególności dla funkcjonowania rynku wewnętrznego. **[Popr. 1]**

(2) Skala***, częstotliwość*** i ~~częstotliwość umyślnych lub przypadkowych~~ ***konsekwencje*** incydentów w obszarze bezpieczeństwa stają się coraz większe i stanowią poważne zagrożenie dla funkcjonowania sieci i systemów informatycznych. ***Systemy te mogą się również stać łatwym celem umyślnych szkodliwych działań, mających na celu uszkodzenie lub przerwanie działania tych systemów.*** Incydenty takie mogą utrudniać prowadzenie działalności gospodarczej, powodować znaczne straty finansowe, podważać zaufanie użytkowników ***i inwestorów*** oraz powodować znaczne straty w gospodarce Unii***, a w konsekwencji stanowić zagrożenie dla dobrobytu obywateli Unii oraz zdolności państw członkowskich do zapewnienia własnej ochrony oraz bezpieczeństwa infrastruktury krytycznej***. **[Popr. 2]**

(3) Jako ponadgraniczne narzędzia komunikacji cyfrowe systemy informatyczne, a przede wszystkim internet, odgrywają istotną rolę w ułatwianiu transgranicznego przepływu towarów, usług i osób. Ze względu na ponadnarodowy charakter tych narzędzi poważne zakłócenia systemów w jednym państwie członkowskim mogą mieć wpływ na pozostałe państwa członkowskie oraz na Unię jako całość. Odporność i stabilność sieci i systemów informatycznych mają zatem zasadnicze znaczenie dla zapewnienia sprawnego funkcjonowania rynku wewnętrznego.

(3a) Zważywszy, że do awarii systemów najczęściej dochodzi nadal z przyczyn niezamierzonych, jak przyczyny naturalne lub błędy ludzkie, infrastruktura powinna być odporna zarówno na zamierzone, jak i niezamierzone zakłócenia, a operatorzy infrastruktury krytycznej powinni projektować systemy oparte na zasadzie odporności. **[Popr. 3]**

(4) Na poziomie Unii należy ustanowić mechanizm współpracy, który umożliwi wymianę informacji i podejmowanie skoordynowanych działań w zakresie ***zapobiegania*** wykrywania i reagowania w odniesieniu do bezpieczeństwa sieci i informacji. Aby mechanizm ten był skuteczny i dostępny dla wszystkich, konieczne jest, by wszystkie państwa członkowskie posiadały minimalne zdolności i strategię zapewniające wysoki poziom bezpieczeństwa sieci i informacji na ich terytorium. Aby promować kulturę wspierającą przeciwdziałanie zagrożeniom i zapewnić zgłaszanie najpoważniejszych incydentów, należy wprowadzić minimalne wymogi w zakresie bezpieczeństwa również w odniesieniu do ~~organów administracji publicznej i~~ ***przynajmniej niektórych rynkowych*** operatorów ~~krytycznej~~ infrastruktury teleinformatycznej. ***Należy zachęcać spółki notowane na giełdzie do dobrowolnego ujawniania incydentów w swoich sprawozdaniach finansowych. Ramy prawne powinny opierać się na potrzebie zabezpieczenia prywatności i integralności obywateli. Sieci ostrzegania o zagrożeniach dla infrastruktury krytycznej należy rozszerzyć na podmioty gospodarcze objęte niniejszą dyrektywą.*** **[Popr. 4]**

(4a) Podczas gdy organy administracji publicznej – z uwagi na swoją misję publiczną – powinny zarządzać własnymi sieciami i systemami informatycznymi oraz chronić je z należytą starannością, niniejsza dyrektywa powinna skupić się na infrastrukturze krytycznej, która ma zasadnicze znaczenie dla utrzymania kluczowych działań gospodarczych i społecznych w dziedzinach energetyki, transportu, bankowości, infrastruktury rynków finansowych i opieki zdrowotnej. Z zakresu niniejszej dyrektywy należy wyłączyć twórców oprogramowania i producentów sprzętu. **[Popr. 5]**

([1]) Dz.U. C 271 z 19.9.2013, s. 133
([2]) Stanowisko Parlamentu Europejskiego z dnia 13 marca 2014 r.

Czwartek, 13 marca 2014 r.

(4b) Współpracę i koordynację między właściwymi organami unijnymi z wysokim przedstawicielem/wiceprzewodniczącym Komisji – odpowiedzialnymi za wspólną politykę zagraniczną i bezpieczeństwa oraz wspólną politykę bezpieczeństwa i obrony – oraz koordynatorem UE ds. zwalczania terroryzmu należy zagwarantować w przypadkach, w których charakter incydentów mających znaczące konsekwencje uważa się za zewnętrzny lub terrorystyczny. **[Popr. 6]**

(5) W celu uwzględnienia wszystkich istotnych incydentów i zagrożeń niniejsza dyrektywa powinna mieć zastosowanie do wszystkich sieci i systemów informatycznych. Obowiązki nałożone na organy administracji publicznej i podmioty gospodarcze nie powinny mieć jednak zastosowania w odniesieniu do przedsiębiorstw udostępniających publiczne sieci łączności lub świadczących publicznie dostępne usługi łączności elektronicznej w rozumieniu dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady ([1]), które podlegają szczególnym wymogom w zakresie bezpieczeństwa i integralności ustanowionym w art. 13a tej dyrektywy, ani nie powinny mieć zastosowania w odniesieniu do dostawców usług zaufania.

(6) Obecne zdolności nie są wystarczające w celu zapewnienia wysokiego poziomu bezpieczeństwa sieci i informacji w Unii. Państwa członkowskie bardzo się różnią pod względem poziomu gotowości, co powoduje rozdrobnienie podejścia w obrębie Unii. Prowadzi to do nierównego poziomu ochrony konsumentów i przedsiębiorstw oraz negatywnie wpływa na ogólny poziom bezpieczeństwa sieci i informacji w Unii. Brak wspólnych minimalnych wymogów dla ~~organów administracji publicznej i~~ podmiotów gospodarczych uniemożliwia z kolei ustanowienie globalnego i skutecznego mechanizmu współpracy na poziomie Unii. ***Uniwersytety i placówki badawcze odgrywają zasadniczą rolę w pobudzaniu badań, rozwoju i innowacyjności w tych obszarach i należy udzielać im odpowiedniego wsparcia finansowego.*** **[Popr. 7]**

(7) Skuteczne reagowanie na wyzwania związane z zapewnieniem bezpieczeństwa sieci i systemów informatycznych wymaga zatem przyjęcia całościowego podejścia na poziomie Unii, które będzie obejmować wprowadzenie wymogów dotyczących budowania i planowania wspólnych minimalnych zdolności, ***rozwijanie dostatecznych umiejętności z zakresu bezpieczeństwa cybernetycznego,*** wymianę informacji i koordynację działań oraz wprowadzenie wspólnych minimalnych wymogów w zakresie bezpieczeństwa ~~dla wszystkich podmiotów gospodarczych, których dotyczy ten problem, oraz dla organów administracji publicznej~~. ***Minimalne wspólne normy należy stosować zgodnie z odpowiednimi zaleceniami grup koordynacji bezpieczeństwa cybernetycznego.*** **[Popr. 8]**

(8) Przepisy niniejszej dyrektywy nie powinny naruszać przysługujących każdemu państwu członkowskiemu praw do wprowadzania niezbędnych środków w celu zapewnienia ochrony podstawowych interesów w zakresie bezpieczeństwa narodowego, do ochrony porządku publicznego i bezpieczeństwa publicznego oraz do zezwalania na prowadzenie dochodzeń dotyczących przestępstw karnych oraz na ich wykrywanie i ściganie. Zgodnie z art. 346 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) żadne państwo członkowskie nie ma obowiązku udzielania informacji, których ujawnienie uznaje za sprzeczne z podstawowymi interesami jego bezpieczeństwa. ***Żadne państwo członkowskie nie ma obowiązku ujawniania niejawnych informacji UE zgodnie z decyzją Rady 2011/292/UE ([2]), informacji objętych postanowieniami umów o zachowaniu poufności lub nieformalnych umów o zachowaniu poufności, takich jak protokół TLP.*** **[Popr. 9]**

(9) W celu osiągnięcia i utrzymania wspólnego wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych każde państwo członkowskie powinno posiadać krajową strategię w zakresie bezpieczeństwa sieci i informacji określającą cele strategiczne i konkretne działania, które należy wdrożyć. Na poziome krajowym należy opracować spełniające zasadnicze wymagania plany współpracy w zakresie bezpieczeństwa sieci i informacji, tak aby osiągnąć poziom zdolności reagowania umożliwiający skuteczną i sprawną współpracę na poziomach krajowym i unijnym w przypadku wystąpienia incydentów***, przy poszanowaniu i ochronie życia prywatnego i danych osobowych. Każde państwo członkowskie powinno zatem być zobowiązane do wypełniania wspólnych norm dotyczących formatu i wymienialności danych, które mają być udostępniane i oceniane. Państwa członkowskie powinny mieć możliwość zwrócenia się do Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) o pomoc w opracowywaniu krajowych strategii w zakresie bezpieczeństwa sieci i informacji na podstawie wspólnej minimalnej strategii w zakresie bezpieczeństwa sieci i informacji.*** **[Popr. 10]**

([1]) Dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa) (Dz.U. L 108 z 24.4.2002, s. 33).

([2]) ***Decyzja Rady 2011/292/UE z dnia 31 marca 2011 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (Dz.U. L 141 z 27.5.2011, s. 17).***

(10) W celu umożliwienia skutecznego wprowadzenia w życie przepisów przyjętych zgodnie z niniejszą dyrektywą w każdym państwie członkowskim należy ustanowić lub wyznaczyć organ odpowiedzialny za koordynowanie kwestii związanych z bezpieczeństwem sieci i informacji oraz działający jako centralny punkt kontaktowy ds. współpracy transgranicznej na poziomie UE. Organom tym należy zapewnić wystarczające zasoby techniczne, finansowe i ludzkie, aby mogły one skutecznie i efektywnie realizować powierzone im zadania w celu osiągnięcia celów niniejszej dyrektywy.

(10a) Z uwagi na różnice w krajowych strukturach zarządzania oraz w celu zabezpieczenia obowiązujących już ustaleń sektorowych lub unijnych organów nadzorczych i regulacyjnych, a także w celu unikania powielania należy umożliwić państwom członkowskim wyznaczanie więcej niż jednego właściwego organu krajowego odpowiedzialnego za realizację zadań związanych z bezpieczeństwem sieci i systemów informatycznych podmiotów gospodarczych objętych niniejszą dyrektywą. Jednak w celu zapewnienia sprawnej współpracy i komunikacji transgranicznej konieczne jest, aby każde państwo członkowskie, bez uszczerbku dla sektorowych ustaleń regulacyjnych, wyznaczyło tylko jeden krajowy pojedynczy punkt kontaktowy odpowiedzialny za współpracę transgraniczną na szczeblu unijnym. Jeżeli wymaga tego struktura konstytucyjna lub inne ustalenia danego państwa członkowskiego, powinno mieć ono prawo do wyznaczenia tylko jednego organu, który będzie wykonywał zadania właściwego organu i pojedynczego punktu kontaktowego. Właściwe organy i krajowe pojedyncze punkty kontaktowe powinny być podmiotami cywilnymi podlegającymi pełnej kontroli demokratycznej i nie powinny wypełniać żadnych zadań w dziedzinie wywiadu, egzekwowania prawa czy obrony ani też być organizacyjnie powiązane w żadnej formie z podmiotami działającymi aktywnie w tych obszarach. **[Popr. 11]**

(11) Wszystkie państwa członkowskie ***i podmioty gospodarcze*** powinny zostać odpowiednio wyposażone, zarówno pod względem zdolności technicznych, jak i możliwości organizacyjnych, w celu zapobiegania incydentom i zagrożeniom dotyczącym sieci i systemów informatycznych, wykrywania ich, reagowania na nie i łagodzenia ich skutków ***w dowolnym momencie***. ***Systemy bezpieczeństwa administracji publicznej powinny być bezpieczne i podlegać demokratycznej kontroli i nadzorowi. Wspólnie wymagane wyposażenie i zdolności powinny odpowiadać wspólnie uzgodnionym normom technicznym oraz standardowym procedurom działania.*** We wszystkich państwach członkowskich należy zatem ustanowić sprawnie funkcjonujące i spełniające zasadnicze wymagania zespoły reagowania na incydenty komputerowe***(CERT)***, które zagwarantują skuteczne i kompatybilne zdolności reagowania na incydenty i zagrożenia oraz zapewnią skuteczną współpracę na poziomie unijnym. ***CERT powinny mieć możliwość interakcji na podstawie wspólnych standardów technicznych i standardowych procedur działania. Z uwagi na różne cechy istniejących CERT, które odpowiadają różnym potrzebom tematycznym i podmiotom, państwa członkowskie powinny zagwarantować, że każdy sektor wymieniony w wykazie podmiotów gospodarczych określonych w niniejszej dyrektywie jest obsługiwany przez co najmniej jeden CERT. W odniesieniu do współpracy transgranicznej CERT państwa członkowskie powinny dopilnować, aby CERT posiadały środki wystarczające do udziału w już działających międzynarodowych i unijnych sieciach współpracy.*** **[Popr. 12]**

(12) Opierając się na znacznych postępach dokonanych w ramach europejskiego forum państw członkowskich (EFMS), które umożliwiły prowadzenie dialogu i wymianę doświadczeń dotyczących sprawdzonych rozwiązań, w tym opracowywanie zasad współpracy na wypadek kryzysów cybernetycznych w Europie, państwa członkowskie i Komisja powinny stworzyć sieć w celu zapewnienia ich stałej komunikacji i wsparcia ich współpracy. Ten bezpieczny i skuteczny mechanizm współpracy***, w którym zapewnia się w stosownych przypadkach udział podmiotów gospodarczych,*** powinien umożliwić uporządkowaną i skoordynowaną wymianę informacji, wykrywanie incydentów oraz reagowanie na nie na poziomie Unii. **[Popr. 13]**

(13) ~~Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (~~ENISA) powinna wspierać działania państw członkowskich i Komisji poprzez zapewnianie wiedzy specjalistycznej i doradztwa oraz poprzez ułatwianie wymiany najlepszych praktyk. W szczególności Komisja ~~powinna~~ ***i państwa członkowskie powinny*** konsultować się z ENISA przy stosowaniu niniejszej dyrektywy. W celu zapewnienia skutecznego i terminowego informowania państw członkowskich i Komisji wczesne ostrzeżenia dotyczące incydentów i zagrożeń należy zgłaszać poprzez sieć współpracy. Aby budować zdolności i wiedzę wśród państw członkowskich, sieć współpracy powinna również służyć jako narzędzie wymiany najlepszych praktyk, pomagać członkom w budowaniu zdolności oraz kierować organizacją wzajemnej weryfikacji i ćwiczeń w zakresie bezpieczeństwa sieci i informacji. **[Popr. 14]**

(13a) W stosownych przypadkach podczas stosowania przepisów niniejszej dyrektywy państwa członkowskie powinny móc wykorzystywać lub dostosowywać istniejące struktury lub strategie organizacyjne. **[Popr. 15]**

Czwartek, 13 marca 2014 r.

(14) Aby umożliwić wymianę szczególnie chronionych i poufnych informacji w ramach sieci współpracy, należy zapewnić bezpieczną infrastrukturę do wymiany informacji. ***W tym celu należy w pełni wykorzystywać istniejące w Unii struktury.*** Bez uszczerbku dla obowiązków związanych ze zgłaszaniem incydentów i zagrożeń o znaczeniu ogólnounijnym w ramach sieci współpracy, dostęp do informacji poufnych z innych państw członkowskich można przyznać wyłącznie tym państwom członkowskim, które wykazały, że ich zasoby i procedury techniczne i finansowe oraz zasoby ludzkie, jak również ich infrastruktura łączności, gwarantują ich skuteczne, sprawne i bezpieczne uczestnictwo w sieci ***przy zastosowaniu przejrzystych metod***. **[Popr. 16]**

(15) Ponieważ większość sieci i systemów informatycznych eksploatowana jest przez podmioty prywatne, niezbędna jest współpraca między sektorem publicznym i prywatnym. Podmioty gospodarcze należy zachęcać do tworzenia własnych nieformalnych mechanizmów współpracy w celu zapewnienia bezpieczeństwa sieci i informacji. Powinny one również współpracować z sektorem publicznym oraz dzielić się ~~z nim~~ ***obustronnie*** informacjami i najlepszymi praktykami ~~w zamian za~~ ***, co obejmuje także wzajemną wymianę odpowiednich informacji,*** wsparcie operacyjne ***i informacje analizowane pod kątem strategicznym*** w przypadku incydentów. ***W celu aktywnego zachęcania do dzielenia się informacjami oraz najlepszymi praktykami konieczne jest zapewnienie, by podmioty gospodarcze uczestniczące w wymianie nie doświadczały strat w wyniku tej współpracy. Konieczne są odpowiednie zabezpieczenia w celu zapewnienia, by tego rodzaju współpraca nie narażała takich podmiotów na wyższe ryzyko braku zgodności lub na nowe zobowiązania na podstawie m.in. prawa konkurencji, własności intelektualnej, ochrony danych czy cyberprzestępczości oraz by nie narażała ich na podwyższone ryzyko operacyjne lub związane z bezpieczeństwem.*** **[Popr. 17]**

(16) W celu zapewnienia przejrzystości i w celu odpowiedniego informowania obywateli ~~UE~~ ***Unii*** i ***unijnych*** podmiotów gospodarczych ~~właściwe organy~~ ***pojedyncze punkty kontaktowe*** powinny założyć wspólną ***ogólnounijną*** stronę internetową, na której publikowane będą niemające poufnego charakteru informacje na temat incydentów***, zagrożeń*** i ~~zagrożeń~~ ***sposobów ich łagodzenia oraz gdzie będzie się udzielać porad dotyczących odpowiedniej obsługi technicznej***. ***Informacje na stronie internetowej powinny być dostępne bez względu na rodzaj urządzenia. Wszelkie dane osobowe publikowane na tej stronie internetowej powinny ograniczać się do tego, co niezbędne, i być jak najbardziej anonimowe.*** **[Popr. 18]**

(17) W przypadku gdy informacje uznaje się za poufne zgodnie z unijnymi i krajowymi przepisami dotyczącymi tajemnicy handlowej, w trakcie wykonywania czynności i realizacji celów określonych w niniejszej dyrektywie należy zapewnić taką poufność.

(18) Na podstawie zwłaszcza krajowych doświadczeń w zarządzaniu kryzysowym i we współpracy z ENISA Komisja i państwa członkowskie powinny opracować unijny plan współpracy w zakresie bezpieczeństwa sieci i informacji określający mechanizmy współpracy ***oraz najlepsze praktyki i wzorce działania*** służące ~~do zwalczania zagrożeń i incydentów~~ ***zapobieganiu zagrożeniom i incydentom oraz ich wykrywaniu, zgłaszaniu i zwalczaniu***. Plan ten należy odpowiednio uwzględniać podczas korzystania z systemu wczesnego ostrzegania w ramach sieci współpracy. **[Popr. 19]**

(19) Przekazywanie wczesnych ostrzeżeń w ramach sieci powinno być wymagane tylko w przypadku, gdy skala i waga danego incydentu lub zagrożenia są lub mogą być w przyszłości na tyle znaczące, że konieczna jest wymiana informacji lub koordynacja reakcji na poziomie Unii. Wczesne ostrzeżenia powinny być zatem ograniczone do ~~rzeczywistych lub potencjalnych~~ incydentów lub zagrożeń, które się szybko rozwijają, przekraczają krajowe zdolności reagowania lub mają wpływ na więcej niż jedno państwo członkowskie. W celu umożliwienia właściwej oceny wszystkie informacje niezbędne do oceny zagrożenia lub incydentu należy przekazywać do sieci współpracy. **[Popr. 20]**

(20) Po otrzymaniu wczesnego ostrzeżenia i dokonaniu jego oceny ~~właściwe organy~~***pojedyncze punkty kontaktowe*** powinny uzgodnić skoordynowaną reakcję zgodnie z unijnym planem współpracy w zakresie bezpieczeństwa sieci i informacji. O środkach przyjętych na poziomie krajowym w wyniku skoordynowanej reakcji należy poinformować ~~właściwe organy~~ ***pojedyncze punkty kontaktowe, ENISA*** oraz Komisję. **[Popr. 21]**

(21) Ze względu na globalny charakter problemów związanych z bezpieczeństwem sieci i informacji istnieje potrzeba zacieśnienia współpracy międzynarodowej w celu poprawy norm bezpieczeństwa i wymiany informacji oraz w celu promowania wspólnego globalnego podejścia w zakresie bezpieczeństwa sieci i informacji. ***Wszelkie ramy takiej współpracy międzynarodowej powinny podlegać przepisom dyrektywy Parlamentu Europejskiego i Rady 95/46/WE*** [1] ***i rozporządzenia (WE) nr 45/2001 Parlamentu Europejskiego i Rady*** [2]**. [Popr. 22]**

(22) Odpowiedzialność za zapewnienie bezpieczeństwa sieci i informacji w dużym stopniu spoczywa na ~~organach administracji publicznej i~~ podmiotach gospodarczych. Za pomocą stosownych wymogów regulacyjnych i dobrowolnych praktyk branżowych należy wspierać i rozwijać kulturę przeciwdziałania zagrożeniom, ***ścisłej współpracy i zaufania,*** obejmującą przeprowadzanie ocen zagrożenia i wdrażanie środków bezpieczeństwa stosownych do ~~danego~~ zagrożenia ***i incydentów, zarówno umyślnych, jak i przypadkowych***. Stworzenie ***godnych zaufania,*** równych warunków działania ma również kluczowe znaczenie dla skutecznego funkcjonowania sieci współpracy w celu zapewnienia skutecznej współpracy ze strony wszystkich państw członkowskich. **[Popr. 23]**

(23) Dyrektywa 2002/21/WE wymaga, by przedsiębiorstwa udostępniające publiczne sieci łączności elektronicznej lub świadczące publicznie dostępne usługi łączności elektronicznej podejmowały odpowiednie środki w celu zabezpieczenia integralności i bezpieczeństwa oraz wprowadza wymogi dotyczące zgłaszania przypadków naruszeń bezpieczeństwa i utraty integralności. Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady ([3]) wymaga od dostawcy publicznie dostępnych usług łączności elektronicznej podjęcia właściwych środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa oferowanych przez siebie usług.

(24) Obowiązki te powinny obejmować nie tylko sektor łączności elektronicznej, lecz również ***operatorów infrastruktury, którzy są w dużym stopniu uzależnieni od technologii informacyjnych i komunikacyjnych i którzy mają kluczowe znaczenie dla utrzymania istotnych funkcji gospodarczych lub społecznych, takich jak dostawy energii elektrycznej i gazu, usługi transportowe, działalność instytucji kredytowych, infrastruktura rynków finansowych i opieka zdrowotna. Zakłócenia tych sieci i systemów informatycznych miałyby wpływ na rynek wewnętrzny. O ile obowiązki ustanowione w niniejszej dyrektywie nie powinny obejmować*** głównych dostawców usług społeczeństwa informacyjnego, określonych w dyrektywie 98/34/WE Parlamentu Europejskiego i Rady ([4]), na których opierają się pochodne usługi społeczeństwa informacyjnego oraz działania w prowadzone w internecie, takie jak platformy handlu elektronicznego, internetowe portale płatnicze, portale społecznościowe, wyszukiwarki, usługi chmur obliczeniowych, ***ogólnie lub*** sklepy z aplikacjami. ~~Zakłócenia tych podstawowych usług społeczeństwa informacyjnego uniemożliwiają świadczenie innych usług społeczeństwa informacyjnego, dla których stanowią one podstawę. Twórcy oprogramowania i producenci sprzętu nie są dostawcami usług społeczeństwa informacyjnego, a zatem nie są oni objęci zakresem powyższych przepisów. Obowiązki te powinny również zostać rozszerzone na organy administracji publicznej oraz operatorów infrastruktury krytycznej, którzy są w dużym stopniu uzależnieni od technologii informacyjnych i komunikacyjnych i którzy mają kluczowe znaczenie dla utrzymania istotnych funkcji gospodarczych i społecznych, takich jak dostawy energii elektrycznej i gazu, usługi transportowe oraz działalność instytucji kredytowych, giełd papierów wartościowych i placówek opieki zdrowotnej. Zakłócenia tych sieci i systemów informatycznych miałyby wpływ na rynek wewnętrzny.~~ ***Podmioty te mogą na zasadzie dobrowolności informować właściwy organ lub pojedynczy punkt kontaktowy o tych incydentach związanych z bezpieczeństwem sieci, które uznają za stosowne. Na ile to możliwe, właściwy organ lub pojedynczy punkt kontaktowy powinien przedstawić podmiotom gospodarczym, które powiadomiły o incydencie, informacje przeanalizowane pod kątem strategicznym, które pomogą przezwyciężyć zagrożenie*** dla ***bezpieczeństwa.*** **[Popr. 24]**

([1]) ***Dyrektywa Parlamentu Europejskiego i Rady 95/46/WE z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. L 281 z 23.11.1995, s. 31).***

([2]) ***Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.U. L 8 z 12.1.2001, s. 1).***

([3]) Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, s. 37).

([4]) Dyrektywa 98/34/WE Parlamentu Europejskiego i Rady z dnia 22 czerwca 1998 r. ustanawiającej procedurę udzielania informacji w dziedzinie norm i przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz.U. L 204 z 21.7.1998, s. 37).

(24a) Podczas gdy dostawcy sprzętu i oprogramowania nie są podmiotami gospodarczymi porównywalnymi z tymi, którzy są objęci niniejszą dyrektywą, ich produkty sprzyjają zapewnieniu bezpieczeństwa sieci i systemów informatycznych. Odgrywają zatem ważną rolę w umożliwieniu podmiotom gospodarczym zabezpieczenia ich infrastruktury sieci i infrastruktury informatycznej. Jako że sprzęt i oprogramowanie podlega już obowiązującym zasadom odpowiedzialności za produkt, państwa członkowskie powinny dopilnować egzekwowania tych zasad. **[Popr. 25]**

(25) Nałożenie na ~~organy administracji publicznej i~~ podmioty gospodarcze obowiązku wprowadzenia środków organizacyjnych i technicznych nie powinno wiązać się z koniecznością zaprojektowania, opracowania i wyprodukowania specjalnego komercyjnego produktu informatycznego w określony sposób. **[Popr. 26]**

(26) ~~Organy administracji publicznej oraz~~ Podmioty gospodarcze powinny zapewnić bezpieczeństwo sieci i systemów, które są pod ich kontrolą. Dotyczy to przede wszystkim sieci i systemów prywatnych, które są zarządzane przez wewnętrzny personel informatyczny lub w przypadku których zapewnienie bezpieczeństwa zlecono na zewnątrz. Wymogi w zakresie bezpieczeństwa i zgłaszania incydentów powinny mieć zastosowanie do odpowiednich podmiotów gospodarczych ~~i organów administracji publicznej~~ bez względu na to, czy one same zapewniają obsługę swoich sieci i systemów informatycznych, czy też zlecają tę obsługę innym podmiotom. **[Popr. 27]**

(27) Aby uniknąć nakładania nieproporcjonalnie dużych obciążeń finansowych i administracyjnych na małe podmioty i na małych użytkowników, wymogi powinny być proporcjonalne do zagrożenia związanego z daną siecią lub danym systemem informatycznym oraz powinny uwzględniać najnowszy stan wiedzy na temat tego rodzaju środków. Wymogi te nie powinny mieć zastosowania w odniesieniu do mikroprzedsiębiorstw.

(28) Właściwe organy ***i pojedyncze punkty kontaktowe*** powinny zwracać należytą uwagę na zachowanie nieformalnych i bezpiecznych kanałów wymiany informacji między podmiotami gospodarczymi i między sektorami publicznym i prywatnym. ***Właściwe organy oraz pojedyncze punkty kontaktowe powinny informować producentów i usługodawców danych produktów i usług ICT o zgłoszonych im incydentach mających znaczące konsekwencje.*** Decyzje o informowaniu społeczeństwa o incydentach zgłoszonych właściwym organom ***i pojedynczym punktom kontaktowym*** należy podejmować przy zachowaniu równowagi między interesem publicznym, zgodnie z którym społeczeństwo powinno być informowane o zagrożeniach, a ryzykiem utraty reputacji i poniesienia szkód handlowych, na jakie narażone są ~~organy administracji publicznej i~~ podmioty gospodarcze zgłaszające incydenty. Wykonując obowiązki w zakresie powiadamiania, właściwe organy ***i pojedyncze punkty kontaktowe*** powinny zwracać szczególną uwagę na potrzebę zachowania poufności w odniesieniu do informacji dotyczących słabych punktów produktów, aż do momentu ~~udostępnienia~~ ***wdrożenia*** stosownych rozwiązań problemów bezpieczeństwa. ***Z zasady pojedyncze punkty kontaktowe nie powinny ujawniać danych osobowych osób zaangażowanych w incydenty. Pojedyncze punkty kontaktowe powinny ujawniać dane osobowe wyłącznie wtedy, kiedy ujawnienie takich danych jest niezbędne i współmierne do celu, w którym są ujawniane.*** **[Popr. 28]**

(29) Właściwe organy powinny dysponować niezbędnymi środkami do wykonywania swoich obowiązków, w tym uprawnieniami do uzyskiwania wystarczających informacji od podmiotów gospodarczych ~~i organów administracji publicznej~~, w celu oceny poziomu bezpieczeństwa sieci i systemów informatycznych, ***zmierzenia liczby, skali i zakresu incydentów,*** jak również wiarygodnymi i pełnymi danymi na temat incydentów, które mają wpływ na funkcjonowanie sieci i systemów informatycznych. **[Popr. 29]**

(30) Źródłem incydentu w wielu przypadkach jest działalność przestępcza. Przestępczy charakter incydentów można podejrzewać nawet wtedy, gdy początkowo dowody nie są wystarczająco przekonujące. W tym kontekście odpowiednia współpraca między właściwymi organami***, pojedynczymi punktami kontaktowymi*** i organami ścigania ~~powinna~~ ***oraz współpraca z EC3 (ośrodek Europolu ds. cyberprzestępczości) i z ENISA powinny*** stanowić część skutecznej i kompleksowej reakcji na zagrożenie związane z możliwością wystąpienia incydentu zagrażającego bezpieczeństwu. Wspieranie rozwoju bezpiecznego, chronionego i bardziej odpornego środowiska wymaga w szczególności systematycznego zgłaszania organom ścigania poważnych incydentów, które mogą mieć charakter przestępczy. Poważne incydenty o charakterze przestępczym należy oceniać w świetle prawa Unii w zakresie cyberprzestępczości. **[Popr. 30]**

(31) W wyniku incydentów w wielu przypadkach istnieje niebezpieczeństwo naruszenia danych osobowych. ***Państwa członkowskie i podmioty gospodarcze powinny chronić przechowywane, przetwarzane i przekazywane dane osobowe przed przypadkowym lub bezprawnym zniszczeniem, przypadkową utratą lub zmianą, a także nieupoważnionym czy bezprawnym przechowywaniem, dostępem, ujawnianiem lub rozpowszechnianiem. Powinny też zapewnić wdrożenie polityki bezpieczeństwa w odniesieniu do przetwarzania danych osobowych.*** W tym kontekście właściwe organy***, pojedyncze punkty kontaktowe*** oraz organy ochrony danych powinny ze sobą współpracować i wymieniać się informacjami ~~dotyczącymi wszystkich istotnych kwestii~~ , w ***stosownych przypadkach z podmiotami gospodarczymi, w*** celu rozwiązywania problemów związanych z przypadkami naruszeń danych osobowych w wyniku incydentów ***zgodnie z mającymi zastosowanie przepisami w dziedzinie ochrony danych.*** ~~Państwa członkowskie powinny wdrożyć~~ ***zgodnie z mającymi zastosowanie przepisami w dziedzinie ochrony danych.*** Obowiązek zgłaszania incydentów zagrażających bezpieczeństwu ***należy wypełniać*** w sposób, który minimalizuje obciążenia administracyjne w przypadku, gdy incydent zagrażający bezpieczeństwu stanowi również naruszenie ***zasad dotyczących*** danych osobowych***, które wymaga zgłoszenia zgodnie z prawem Unii*** w ~~rozumieniu rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w~~ zakresie ~~przetwarzania~~ ***ochrony*** danych ~~osobowych i swobodnego przepływu tych danych ([1]). Współpracując z właściwymi organami i organami ochrony danych, ENISA mogłaby opracować~~ ***ENISA powinna udzielić pomocy, opracowując*** mechanizmy ~~i wzory formularzy na potrzeby~~ wymiany informacji~~, dzięki czemu nie byłoby konieczne stosowanie dwóch formularzy. Pojedynczy formularz ułatwiłby~~ ***i jednolity wzór formularza***, ***które ułatwiłyby*** zgłaszanie incydentów~~, które stanowią~~ ***stanowiących*** naruszenie danych osobowych, zmniejszając tym samym obciążenia administracyjne dla przedsiębiorstw i organów administracji publicznej. **[Popr. 31]**

(32) Normalizacja wymogów w zakresie bezpieczeństwa jest ***dobrowolnym*** procesem napędzanym przez rynek***, który powinien umożliwić podmiotom gospodarczym korzystanie z alternatywnych środków w celu osiągnięcia co najmniej podobnych wyników***. W celu zapewnienia spójnego stosowania norm bezpieczeństwa państwa członkowskie powinny wspierać dążenie do zgodności lub zbieżności z określonymi ***interoperacyjnymi*** normami w celu zapewnienia wysokiego poziomu bezpieczeństwa na poziomie Unii. W tym celu ~~konieczne~~ ***należy rozważyć stosowanie otwartych norm międzynarodowych do bezpieczeństwa sieci i informacji lub opracowanie takich narzędzi. Kolejnym koniecznym krokiem naprzód*** może być przygotowanie ujednoliconych norm, czego należy dokonać zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1025/2012 ([2]). ***W szczególności należy upoważnić ETSI, CEN i CENELEC do proponowania skutecznych i wydajnych otwartych unijnych norm bezpieczeństwa, w których unika się preferencji technologicznych w jak najwyższym stopniu i którymi mogą łatwo zarządzać małe i średnie podmioty gospodarcze. Normy międzynarodowe dotyczące bezpieczeństwa cybernetycznego należy dokładnie sprawdzić w celu zapewnienia, że nie zostały one naruszone, ustanawiają odpowiednie poziomy bezpieczeństwa, tym samym gwarantując, że zalecona zgodność z normami bezpieczeństwa cybernetycznego zwiększa, a nie zmniejsza ogólny poziom tego bezpieczeństwa w Unii.*** **[Popr. 32]**

(33) Komisja powinna okresowo dokonywać przeglądu niniejszej dyrektywy, ***w drodze konsultacji ze wszystkimi zainteresowanymi stronami,*** w szczególności w celu sprawdzenia, czy konieczne jest wprowadzenie zmian w świetle zmieniających się technologii i warunków ***społecznych, politycznych lub*** rynkowych. **[Popr. 33]**

(34) W celu umożliwienia prawidłowego funkcjonowania sieci współpracy należy przekazać Komisji uprawnienia do przyjęcia aktów zgodnie z art. 290 TFUE w odniesieniu do ~~określenia kryteriów, które państwo członkowskie musi spełnić, aby móc uczestniczyć w bezpiecznym systemie~~ ***wspólnego zestawu norm w zakresie wzajemnych połączeń i bezpieczeństwa dla potrzeb bezpiecznej infrastruktury służącej do*** wymiany informacji, sprecyzowania, które zdarzenia wymagają wczesnego ostrzegania~~, a także określenia okoliczności, w których podmioty gospodarcze i organy administracji publicznej są zobowiązane do zgłaszania incydentów~~. **[Popr. 34]**

([1]) ~~SEC(2012) 72 final.~~

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniającym dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylającym decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE (Dz.U. L 316 z 14.11.2012, s. 12).

(35) Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów. Przygotowując i opracowując akty delegowane, Komisja powinna zapewnić jednoczesne, terminowe i odpowiednie przekazywanie stosownych dokumentów Parlamentowi Europejskiemu i Radzie.

(36) W celu zapewnienia jednolitych warunków wykonywania niniejszej dyrektywy należy powierzyć Komisji uprawnienia wykonawcze w zakresie współpracy między ~~właściwymi organami~~ ***pojedynczymi punktami kontaktowymi*** i Komisją w ramach sieci współpracy, ~~dostępu do bezpiecznej infrastruktury służącej do wymiany informacji,~~ ***(bez uszczerbku dla istniejących mechanizmów współpracy na szczeblu krajowym)*** unijnego planu współpracy w zakresie bezpieczeństwa sieci i informacji, ***a także*** formatów i procedur mających zastosowanie wobec wymogów dotyczących ~~informowania społeczeństwa o incydentach, oraz norm lub specyfikacji technicznych dotyczących bezpieczeństwa sieci i informacji~~ ***zgłaszania incydentów mających znaczące konsekwencje***. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 ([1]). **[Popr. 35]**

(37) Przy stosowaniu niniejszej dyrektywy Komisja powinna w stosownych przypadkach współpracować z odpowiednimi komitetami sektorowymi i odpowiednimi organami ustanowionymi na poziomie ~~UE~~ ***Unii***, zwłaszcza w dziedzinie ***administracji elektronicznej,*** energetyki, transportu ~~i~~ , opieki zdrowotnej ***i obrony***. **[Popr. 36]**

(38) Informacjami, które właściwy organ ***lub pojedynczy punkt kontaktowy*** uznaje za poufne zgodnie z unijnymi i krajowymi przepisami dotyczącymi tajemnicy handlowej, można się wymieniać z Komisją ~~i~~ ***, jej odpowiednimi agencjami,*** innymi ***pojedynczymi punktami kontaktowymi i/lub innymi*** właściwymi organami ***krajowymi*** tylko wtedy, gdy wymiana taka jest absolutnie niezbędna w celu wykonania niniejszej dyrektywy. Ujawnione informacje powinny ograniczać się do tego, co jest ~~właściwe~~ ***istotne, niezbędne*** i proporcjonalne do celów takiej wymiany informacji***, oraz być zgodne z ustalonymi wcześniej kryteriami poufności i bezpieczeństwa, na mocy decyzji Rady 2011/292/UE, do informacji objętych postanowieniami umów o zachowaniu poufności i nieformalnych umów o zachowaniu poufności, takich jak protokół TLP.*** **[Popr. 37]**

(39) Wymiana informacji dotyczących zagrożeń i incydentów w ramach sieci współpracy i zapewnienie zgodności z wymogami dotyczącymi zgłaszania incydentów właściwym organom krajowym ***lub pojedynczym punktom kontaktowym*** mogą oznaczać konieczność przetwarzania danych osobowych. Takie przetwarzanie danych osobowych jest niezbędne do realizacji celów niniejszej dyrektywy będących w interesie publicznym i w związku z tym jest uzasadnione na mocy art. 7 dyrektywy 95/46/WE. Nie stanowi ono, w odniesieniu do tych uzasadnionych celów, nieproporcjonalnej i niedopuszczalnej ingerencji naruszającej istotę prawa do ochrony danych osobowych, które gwarantuje art. 8 Karty praw podstawowych Unii Europejskiej. Przy wdrażaniu niniejszej dyrektywy zastosowanie powinno mieć, w stosownych przypadkach, rozporządzenie (WE) nr 1049/2001 Parlamentu Europejskiego i Rady ([2]). W przypadku gdy dane są przetwarzane przez instytucje i organy Unii, tego rodzaju przetwarzanie w celu wprowadzenia niniejszej dyrektywy w życie powinno być zgodne z rozporządzeniem (WE) nr 45/2001. **[Popr. 38]**

(40) Ponieważ cel niniejszej dyrektywy, to jest zapewnienie wysokiego poziomu bezpieczeństwa sieci i informacji w Unii, nie może zostać osiągnięty w wystarczającym stopniu przez państwa członkowskie działające samodzielnie, natomiast z uwagi na skutki proponowanego działania możliwe jest lepsze jego osiągnięcie na poziomie unijnym, Unia może podjąć działania zgodnie z zasadą pomocniczości, o której mowa w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsza dyrektywa nie wykracza poza to, co jest konieczne do osiągnięcia tych celów.

(41) Niniejsza dyrektywa jest zgodna z prawami podstawowymi i zasadami uznanymi w Karcie praw podstawowych Unii Europejskiej, a w szczególności zasadami dotyczącymi prawa do poszanowania życia prywatnego i komunikowania się, prawa do ochrony danych osobowych i wolności prowadzenia działalności gospodarczej, prawa własności, prawa do skutecznego środka prawnego i prawa do bycia wysłuchanym. Niniejszą dyrektywę należy wdrażać zgodnie z tymi prawami i zasadami.

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiającym przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.U. L 55 z 28.2.2011, s. 13).

([2]) Rozporządzenie (WE) nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji (Dz.U. L 145 z 31.5.2001, s. 43).

(41a) Zgodnie ze wspólną deklaracją polityczną państw członkowskich i Komisji dotyczącą dokumentów wyjaśniających z dnia 28 września 2011 r. państwa członkowskie zobowiązały się dołączać, w uzasadnionych przypadkach, do powiadomienia o środkach transpozycji jeden lub większą liczbę dokumentów wyjaśniających związki między elementami dyrektywy a odpowiadającymi im częściami krajowych instrumentów służących transpozycji. W odniesieniu do niniejszej dyrektywy ustawodawca uznaje, że przekazanie takich dokumentów jest uzasadnione. **[Popr. 39]**

(41b) Zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 skonsultowano się z Europejskim Inspektorem Ochrony Danych Osobowych, który wydał opinię w dniu 14 czerwca 2013 r. ([1]),

PRZYJMUJĄ NINIEJSZĄ DYREKTYWĘ:

ROZDZIAŁ I

PRZEPISY OGÓLNE

Artykuł 1

Przedmiot i zakres zastosowania

1. Niniejsza dyrektywa ustanawia środki w celu zapewnienia wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii.

2. W tym celu niniejsza dyrektywa:

a) określa obowiązki dla wszystkich państw członkowskich w zakresie zapobiegania zagrożeniom i incydentom dotyczącym sieci i systemów informatycznych, postępowania w przypadku ich wystąpienia oraz reagowania na nie;

b) ustanawia mechanizm współpracy między państwami członkowskimi w celu zapewnienia jednolitego stosowania niniejszej dyrektywy w obrębie Unii oraz, w razie konieczności, w celu zapewnienia skoordynowanego ~~i~~ , sprawnego ***i skutecznego*** postępowania w przypadku wystąpienia zagrożeń i incydentów dotyczących sieci i systemów informatycznych oraz reagowania na nie; **[Popr. 40]**

c) ustanawia wymogi w zakresie bezpieczeństwa dla podmiotów gospodarczych ~~i organów administracji publicznej~~. **[Popr. 41]**

3. Wymogi bezpieczeństwa przewidziane w art. 14 niniejszej dyrektywy nie mają zastosowania do przedsiębiorstw udostępniających publiczne sieci łączności lub świadczących publicznie dostępne usługi łączności elektronicznej w rozumieniu dyrektywy 2002/21/WE, które to przedsiębiorstwa muszą spełniać szczególne wymogi w zakresie bezpieczeństwa i integralności określone w art. 13a i 13b tej dyrektywy, ani do dostawców usług zaufania.

4. Niniejszą dyrektywę stosuje się bez uszczerbku dla unijnych przepisów dotyczących cyberprzestępczości oraz dyrektywy Rady 2008/114/WE ([2]).

5. Niniejsza dyrektywa pozostaje również bez uszczerbku dla dyrektywy 95/46/WE, dyrektywy 2002/58/WE oraz rozporządzenia ***(WE) nr 45/2001***. ***Wszelkie wykorzystanie danych osobowych ogranicza się do tego, co jest absolutnie niezbędne dla celów niniejszej dyrektywy, a dane te są anonimowe, jeśli nie zupełnie, to w jak największym stopniu.*** **[Popr. 42]**

6. Wymiana informacji w ramach sieci współpracy na mocy rozdziału III i zgłaszanie incydentów dotyczących bezpieczeństwa sieci i informacji na mocy art. 14 mogą wymagać przetwarzania danych osobowych. Państwo członkowskie zezwala na takie przetwarzanie, które jest niezbędne do realizacji celów niniejszej dyrektywy będących w interesie publicznym, zgodnie z ustawodawstwem krajowym implementującym art. 7 dyrektywy 95/46/WE i dyrektywę 2002/58/WE.

([1]) Dz.U. C 32 z 4.2.2014, s. 19.
([2]) Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz.U. L 345 z 23.12.2008, s. 75).

Artykuł 1a

Ochrona i przetwarzanie danych osobowych;

1. Wszelkie przetwarzanie danych osobowych w państwach członkowskich na mocy niniejszej dyrektywy odbywa się zgodnie z dyrektywą 95/46/WE i dyrektywą 2002/58/WE.

2. Wszelkie przetwarzanie danych osobowych przez Komisję i ENISA na mocy niniejszego rozporządzenia odbywa się zgodnie z rozporządzeniem (WE) nr 45/2001.

3. Wszelkie przetwarzanie danych osobowych przez działające przy Europolu Centrum ds. Walki z Cyberprzestępczością do celów niniejszej dyrektywy odbywa się na mocy decyzji Rady 2009/371/WSiSW [1].

4. Przetwarzanie danych osobowych jest uczciwe i zgodne z prawem oraz ściśle ograniczone do minimalnych danych niezbędnych do celów, w których odbywa się ich przetwarzanie. Są one przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez czas nie dłuższy niż jest to konieczne do celów, w których dane osobowe są przetwarzane.

5. Zgłaszanie incydentów, o którym mowa w art. 14 niniejszej dyrektywy, pozostaje bez uszczerbku dla określonych w art. 4 dyrektywy 2002/58/WE i w rozporządzeniu Komisji (UE) nr 611/2013 [2] ***przepisów i obowiązków dotyczących powiadamiania o przypadkach naruszenia danych osobowych.*** **[Popr. 43]**

Artykuł 2

Minimalna harmonizacja

Państwa członkowskie mają prawo przyjmowania lub utrzymania w mocy przepisów zapewniających wyższy poziom bezpieczeństwa, bez uszczerbku dla ich zobowiązań wynikających z prawa unijnego.

Artykuł 3

Definicje

Do celów niniejszej dyrektywy stosuje się następujące definicje:

1) „sieci i systemy informatyczne" oznaczają:

   a) sieci łączności elektronicznej w rozumieniu dyrektywy 2002/21/WE, oraz

   b) wszelkie urządzenia lub grupy połączonych lub powiązanych urządzeń, z których jedno lub więcej, zgodnie z oprogramowaniem, dokonuje automatycznego przetwarzania danych ~~komputerowych~~ ***cyfrowych***, jak również **[Popr. 44]**

   c) dane ~~komputerowe~~ ***cyfrowe*** przechowywane, przetwarzane, odzyskiwane lub przekazywane przez elementy określone w lit. a) i b) w celu ich eksploatacji, użycia, ochrony lub utrzymania; **[Popr. 45]**

2) „bezpieczeństwo" oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na zdarzenia przypadkowe lub działania złośliwe naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przekazywanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy; ***„bezpieczeństwo" obejmuje odpowiednie urządzenia techniczne, rozwiązania i procedury operacyjne spełniające wymogi bezpieczeństwa określone w niniejszej dyrektywie;*** **[Popr. 46]**

---

[1] ***Decyzja Rady 2009/371/WSiSW z dnia 6 kwietnia 2009 r. ustanawiająca Europejski Urząd Policji (Europol) (Dz.U. L 121 z 15.5.2009, s. 37).***

[2] ***Rozporządzenie Komisji (UE) nr 611/2013 z dnia 24 czerwca 2013 r. w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady o prywatności i łączności elektronicznej (Dz.U. L 173 z 26.6.2013, s. 2).***

3) „zagrożenie" oznacza każdą ***dającą się racjonalnie określić*** okoliczność lub zdarzenie, które mogą mieć niekorzystny wpływ na bezpieczeństwo; **[Popr. 47]**

4) „incydent" oznacza ~~każdą okoliczność lub~~ ***każde*** zdarzenie, które ~~mają~~ ***ma*** rzeczywisty niekorzystny wpływ na bezpieczeństwo; **[Popr. 48]**

~~5) „usługi społeczeństwa informacyjnego" oznaczają usługę w rozumieniu art. 1 pkt 2) dyrektywy 98/34/WE;~~ **[Popr. 49]**

6) „plan współpracy w zakresie bezpieczeństwa sieci i informacji" oznacza plan zawierający ramy dla funkcji, obowiązków i procedur organizacyjnych mających na celu utrzymanie lub przywrócenie funkcjonowania sieci i systemów informatycznych, w przypadku wystąpienia zagrożenia lub incydentu, które ich dotyczą;

7) „postępowanie w przypadku incydentu" oznacza wszystkie procedury umożliwiające ***wykrycie incydentu, zapobieżenie mu, jego*** analizę i ograniczenie ***jego*** skutków ~~incydentu~~ oraz reakcję na niego; **[Popr. 50]**

8) „podmiot gospodarczy" oznacza:

~~a) dostawcę usług społeczeństwa informacyjnego umożliwiających świadczenie innych usług społeczeństwa informacyjnego, których niewyczerpujący wykaz zamieszczony jest w załączniku II;~~ **[Popr. 51]**

b) operatora infrastruktury ~~krytycznej~~, która ma zasadnicze znaczenie dla utrzymania kluczowych działań gospodarczych i społecznych w dziedzinach energetyki, transportu, bankowości, ~~obrotu papierami wartościowymi~~ ***infrastruktury rynków finansowych, internetowych punktów wymiany, łańcucha dostaw żywności*** i opieki zdrowotnej, ~~których~~ ***a której uszkodzenie lub zniszczenie miałoby poważny wpływ na dane państwo członkowskie w postaci braku możliwości utrzymania tych funkcji (ich*** niewyczerpujący wykaz zamieszczony jest w załączniku II. ***), o ile dane sieci i systemy informatyczne są powiązane z jego podstawowymi usługami;*** **[Popr. 52]**

8a) „incydent mający znaczące konsekwencje" oznacza incydent mający wpływ na bezpieczeństwo i ciągłość sieci informatycznej lub systemu informatycznego, który prowadzi do poważnego zakłócenia istotnych funkcji gospodarczych lub społecznych; **[Popr. 53]**

9) „norma" oznacza normę, o której mowa w rozporządzeniu (UE) nr 1025/2012;

10) „specyfikacja" oznacza specyfikację, o której mowa w rozporządzeniu (UE) nr 1025/2012;

11) „dostawca usług zaufania" oznacza każdą osobę fizyczną lub prawną, która świadczy jakąkolwiek elektroniczną usługę polegającą na tworzeniu, kontroli, walidacji i przechowywaniu podpisów elektronicznych, pieczęci elektronicznych, elektronicznych znaczników czasu, dokumentów elektronicznych, usług doręczenia elektronicznego, usług uwierzytelniania witryn internetowych i certyfikatów elektronicznych, w tym certyfikatów podpisów elektronicznych i pieczęci elektronicznych;

11a) „rynek regulowany" oznacza rynek regulowany w rozumieniu art. 4 pkt 14 dyrektywy 2004/39/WE Parlamentu Europejskiego i Rady ([1])**;** **[Popr. 54]**

11b) „wielostronna platforma obrotu (MTF)" oznacza wielostronną platformę obrotu w rozumieniu art. 4 pkt 15 dyrektywy 2004/39/WE; **[Popr. 55]**

11c) „zorganizowana platforma obrotu" oznacza wielostronny system lub wielostronną platformę, niebędące rynkiem regulowanym, wielostronną platformą obrotu ani centralnym kontrahentem, obsługiwane przez przedsiębiorstwo inwestycyjne lub podmiot gospodarczy, w ramach których umożliwia się wzajemne powiązanie w obrębie systemu interesów licznych stron trzecich w zakresie kupna i sprzedaży obligacji, strukturyzowanych produktów finansowych, uprawnień do emisji lub instrumentów pochodnych w sposób skutkujący zawarciem kontraktu, zgodnie z tytułem II dyrektywy 2004/39/WE. **[Popr. 56]**

([1]) ***Dyrektywa 2004/39/WE Parlamentu Europejskiego i Rady z dnia 21 kwietnia 2004 r. w sprawie rynków instrumentów finansowych (Dz.U. L 45 z 16.2.2005, s. 18).***

Czwartek, 13 marca 2014 r.

ROZDZIAŁ II

RAMY KRAJOWE W ZAKRESIE BEZPIECZEŃSTWA SIECI I INFORMACJI

Artykuł 4

Zasada

Państwa członkowskie zapewniają wysoki poziom bezpieczeństwa sieci i systemów informatycznych na swoim terytorium zgodnie z niniejszą dyrektywą.

Artykuł 5

Krajowa strategia w zakresie bezpieczeństwa sieci i informacji oraz krajowy plan współpracy w zakresie bezpieczeństwa sieci i informacji

1. Każde państwo członkowskie przyjmuje krajową strategię w zakresie bezpieczeństwa sieci i informacji określającą cele strategiczne i konkretne środki polityczne i regulacyjne mające na celu osiągnięcie i utrzymanie wysokiego poziomu bezpieczeństwa sieci i informacji. Krajowa strategia w zakresie bezpieczeństwa sieci i informacji uwzględnia zwłaszcza następujące kwestie:

a) określenie celów i priorytetów strategii w oparciu o aktualną analizę zagrożeń i incydentów;

b) ramy zarządzania służące realizacji celów i priorytetów strategii, w tym jasne określenie funkcji i zakresu obowiązków organów rządowych i innych właściwych podmiotów;

c) określenie ogólnych środków w zakresie gotowości, reagowania i przywracania stanu normalnego, w tym mechanizmów współpracy pomiędzy sektorami publicznym i prywatnym;

d) wstępne określenie programów edukacyjnych, informacyjnych i szkoleniowych;

e) plany w zakresie badań i rozwoju oraz opis, w jaki sposób plany te odzwierciedlają wyznaczone priorytety;

ea) Państwa członkowskie mogą zwrócić się do ENISA o pomoc w opracowywaniu krajowych strategii w zakresie bezpieczeństwa sieci i informacji oraz krajowych planów współpracy w zakresie bezpieczeństwa sieci i informacji na podstawie wspólnej minimalnej strategii w zakresie bezpieczeństwa sieci i informacji. **[Popr. 57]**

2. Krajowa strategia w zakresie bezpieczeństwa sieci i informacji obejmuje krajowy plan współpracy w zakresie bezpieczeństwa sieci i informacji, spełniający co najmniej następujące wymogi:

a) opracowanie ~~planu oceny zagrożeń umożliwiającego~~ ***ram zarządzania ryzykiem w celu stworzenia metodyki obejmującej*** określenie zagrożeń***, ustalenie stopnia ich ważności, ich ocenę*** i ***postępowanie w przypadku ich wystąpienia,*** ocenę wpływu potencjalnych incydentów ***i sposoby zapobiegania i kontroli, a także w celu określenia kryteriów wyboru możliwych środków zaradczych***; **[Popr. 58]**

b) określenie funkcji i zakresu obowiązków poszczególnych ***organów i innych*** podmiotów zaangażowanych ~~w realizację planu~~ ***we wdrażanie tych ram***; **[Popr. 59]**

c) określenie procedur współpracy i komunikacji zapewniających zapobieganie, wykrywanie, reagowanie, naprawę i przywrócenie stanu normalnego, zgodnie z poziomem stanu alarmowego;

d) opracowanie planu dotyczącego ćwiczeń i szkoleń w zakresie bezpieczeństwa sieci i informacji, mającego na celu ulepszenie, zatwierdzenie i sprawdzenie planu. Wyciągnięte wnioski są udokumentowywane i włączane do zaktualizowanych wersji planu.

3. Krajową strategię w zakresie bezpieczeństwa sieci i informacji oraz krajowy plan współpracy w zakresie bezpieczeństwa sieci i informacji są przekazywane Komisji w ciągu ~~jednego miesiąca~~ ***trzech miesięcy*** od ich przyjęcia. **[Popr. 60]**

Artykuł 6

~~Właściwy organ krajowy~~ ***Właściwe organy krajowe i krajowe pojedyncze punkty kontaktowe*** ds. bezpieczeństwa sieci i systemów informatycznych **[Popr. 61]**

1. Każde państwo członkowskie wyznacza ***co najmniej jeden cywilny*** właściwy organ krajowy ds. bezpieczeństwa sieci i systemów informatycznych (~~„właściwy organ”~~ „***właściwy organem lub właściwe organy***”). **[Popr. 62]**

2. Właściwe organy monitorują stosowanie niniejszej dyrektywy na poziomie krajowym oraz przyczyniają się do jej jednolitego stosowania w całej Unii.

2a. Jeżeli państwo członkowskie wyznacza więcej niż jeden właściwy organ, wyznacza ono krajowy organ cywilny, np. właściwy organ, jako pojedynczy krajowy punkt kontaktowy ds. bezpieczeństwa sieci i systemów informatycznych („pojedynczy punkt kontaktowy”). Jeżeli państwo członkowskie wyznacza tylko jeden właściwy organ, organ ten jest również pojedynczym punktem kontaktowym. **[Popr. 63]**

2b. Właściwe organy i pojedynczy punkt kontaktowy tego samego państwa członkowskiego ściśle ze sobą współpracują w zakresie obowiązków określonych w niniejszej dyrektywie. **[Popr. 64]**

2c. Pojedynczy punkt kontaktowy zapewnia współpracę transgraniczną z innymi pojedynczymi punktami kontaktowymi. **[Popr. 65]**

3. Państwa członkowskie zapewniają właściwym organom ***i pojedynczym punktom kontaktowym*** odpowiednie zasoby techniczne, finansowe i ludzkie, aby mogły one skutecznie i efektywnie realizować powierzone im zadania w celu osiągnięcia celów niniejszej dyrektywy. Państwa członkowskie zapewniają skuteczną, efektywną i bezpieczną współpracę ~~właściwych organów~~ ***pojedynczych punktów kontaktowych*** za pośrednictwem sieci, o której mowa w art. 8. **[Popr. 66]**

4. Państwa członkowskie dopilnowują, by właściwe organy ***i pojedyncze punkty kontaktowe – w stosownych przypadkach zgodnie z ust. 2a niniejszego artykułu –*** otrzymywały od ~~organów administracji publicznej i~~ podmiotów gospodarczych zgłoszenia dotyczące incydentów określone w art. 14 ust. 2 oraz posiadały uprawnienia w zakresie wykonywania i egzekwowania przepisów, o których mowa w art. 15. **[Popr. 67]**

4a. Jeżeli prawo Unii przewiduje dla danego sektora unijny organ nadzorczy lub regulacyjny, między innymi w zakresie bezpieczeństwa sieci i systemów informatycznych, zgodnie z art. 14 ust. 2, organ ten otrzymuje zgłoszenia incydentów od zainteresowanych podmiotów gospodarczych z tego sektora oraz posiada uprawnienia w zakresie wdrażania i egzekwowania, o których mowa w art. 15. Ten organ unijny ściśle współpracuje w zakresie tych obowiązków z właściwymi organami i pojedynczym punktem kontaktowym przyjmującego państwa członkowskiego. Pojedynczy punkt kontaktowy przyjmującego państwa członkowskiego reprezentuje organ unijny w odniesieniu do obowiązków określonych w rozdziale III. **[Popr. 68]**

5. W stosownych przypadkach właściwe organy ***i pojedyncze punkty kontaktowe*** konsultują się i współpracują z odpowiednimi krajowymi organami ścigania i z organami ochrony danych. **[Popr. 69]**

6. Każde państwo członkowskie powiadamia niezwłocznie Komisję o wyznaczeniu ~~właściwego organu~~ ***właściwych organów i pojedynczego punktu kontaktowego***, o ~~jego~~ ***ich*** zadaniach i o ***dotyczących ich*** wszelkich późniejszych zmianach ~~dotyczących tego organu~~. Każde państwo członkowskie podaje do publicznej wiadomości informację o wyznaczeniu ~~swojego właściwego organu~~ ***właściwych organów***. **[Popr. 70]**

Artykuł 7

Zespół reagowania na incydenty komputerowe

1. Każde państwo członkowskie ustanawia ***przynajmniej jeden*** zespół reagowania na incydenty komputerowe („CERT”) ***dla każdego sektora określonego w załączniku II***, odpowiedzialny za postępowanie w przypadku wystąpienia incydentów i zagrożeń według jasno określonej procedury, która jest zgodna z wymogami określonymi w załączniku I pkt 1. CERT może zostać ustanowiony w ramach właściwego organu. **[Popr. 71]**

2. Państwa członkowskie zapewniają CERT odpowiednie zasoby techniczne, finansowe i ludzkie, aby mogły one skutecznie realizować zadania określone w załączniku I pkt 2.

3. Państwa członkowskie dopilnowują, by CERT wykorzystywały bezpieczną i odporną infrastrukturę komunikacyjną i informacyjną na poziomie krajowym, która jest kompatybilna i interoperacyjna z bezpiecznym systemem wymiany informacji, o którym mowa w art. 9.

4. Państwa członkowskie powiadamiają Komisję o zasobach i mandacie CERT, jak również o ich procedurach postępowania w przypadku incydentów.

5. CERT ~~działa~~ ***działają*** pod nadzorem właściwego organu ***lub pojedynczego punktu kontaktowego***, który regularnie dokonuje przeglądu stosowności ~~jego~~ ***ich*** zasobów, ~~jego mandatu~~ ***mandatów*** oraz skuteczności ~~jego~~ ***ich*** procedury postępowania w przypadku incydentów. **[Popr. 72]**

5a. Państwa członkowskie zapewniają CERT odpowiednie zasoby ludzkie i finansowe, aby mogły one czynnie uczestniczyć w międzynarodowych, a zwłaszcza unijnych, sieciach współpracy. **[Popr. 73]**

5b. CERT są uprawnione i zachęcane do inicjowania wspólnych ćwiczeń z innymi CERT, ze wszystkimi CERT państw członkowskich oraz z właściwymi instytucjami państw trzecich, a także z CERT instytucji wielonarodowych i międzynarodowych, takich jak Organizacja Traktatu Północnoatlantyckiego czy Organizacja Narodów Zjednoczonych, oraz do udziału w takich wspólnych ćwiczeniach. **[Popr. 74]**

5c. Państwa członkowskie mogą zwrócić się do ENISA lub do innych państw członkowskich o pomoc w rozwijaniu krajowych CERT. **[Popr. 75]**

ROZDZIAŁ III

WSPÓŁPRACA MIĘDZY WŁAŚCIWYMI ORGANAMI

Artykuł 8

Sieć współpracy

1. ~~Właściwe organy i~~ ***Pojedyncze punkty kontaktowe,*** Komisja ***i ENISA*** ustanawiają sieć („***sieć*** współpracy") służącą do współpracy w zakresie przeciwdziałania zagrożeniom i incydentom dotyczącym sieci i systemów informatycznych. **[Popr. 76]**

2. Sieć współpracy umożliwia stałą łączność między Komisją a ~~właściwymi organami~~ ***pojedynczymi punktami kontaktowymi***. ***ENISA wspiera,*** na żądanie ~~Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA) wspiera~~ , sieć współpracy poprzez zapewnianie wiedzy specjalistycznej i doradztwa. ***W stosownych przypadkach podmioty gospodarcze i dostawcy rozwiązań z zakresu bezpieczeństwa cybernetycznego mogą również zostać zaproszeni do uczestnictwa w działaniach sieci współpracy, o której mowa w ust. 3 lit. g) oraz i).***

W stosownych przypadkach sieć współpracy współpracuje z organami ochrony danych.

Komisja regularnie informuje sieć współpracy o badaniach dotyczących bezpieczeństwa oraz innych stosownych programach programu „Horyzont 2020". **[Popr. 77]**

3. W ramach sieci współpracy ~~właściwe organy~~ ***pojedyncze punkty kontaktowe***:

a) przekazują wczesne ostrzeżenia dotyczące zagrożeń i incydentów zgodnie z art. 10;

b) zapewniają skoordynowaną reakcję zgodnie z art. 11;

c) regularnie publikują na wspólnej stronie internetowej niemające poufnego charakteru informacje na temat aktualnych wczesnych ostrzeżeń i skoordynowanych reakcji;

d) wspólnie omawiają i oceniają~~, na wniosek państwa członkowskiego lub Komisji,~~ jedną krajową strategię w zakresie bezpieczeństwa sieci i informacji, lub ich większą liczbę, lub jeden krajowy plan współpracy w zakresie bezpieczeństwa sieci i informacji, lub ich większą liczbę, o których mowa w art. 5, w zakresie niniejszej dyrektywy;

e) wspólnie omawiają i oceniają~~, na wniosek państwa członkowskiego lub Komisji,~~ skuteczność CERT, zwłaszcza w przypadku gdy ćwiczenia w zakresie bezpieczeństwa sieci i informacji przeprowadzane są na poziomie unijnym;

f) współpracują i wymieniają się ~~informacjami dotyczącymi wszystkich~~ ***wiedzą specjalistyczną na temat*** istotnych kwestii z ***zakresu bezpieczeństwa sieci i informacji, w szczególności w dziedzinach ochrony danych, energetyki, transportu, bankowości, rynków finansowych i opieki zdrowotnej,*** z działającym przy Europolu Europejskim Centrum ds. Walki z Cyberprzestępczością oraz z innymi właściwymi organami europejskimi~~, w szczególności w dziedzinach ochrony danych, energetyki, transportu, bankowości, obrotu papierami wartościowymi i opieki zdrowotnej~~;

fa) w stosownych przypadkach przekazują w drodze sprawozdań informacje koordynatorowi UE ds. zwalczania terroryzmu i mogą zwrócić się o pomoc związaną z analizą, pracami przygotowawczymi i działaniami sieci współpracy;

g) wymieniają się informacjami i najlepszymi praktykami między sobą i z Komisją oraz udzielają sobie wzajemnie pomocy w budowaniu zdolności w zakresie bezpieczeństwa sieci i informacji;

~~h) regularnie organizują wzajemne oceny zdolności i gotowości;~~

i) organizują ćwiczenia w zakresie bezpieczeństwa sieci i informacji na poziomie unijnym oraz uczestniczą, w stosownych przypadkach, w międzynarodowych ćwiczeniach w zakresie bezpieczeństwa sieci i informacji;

ia) angażują podmioty gospodarcze, konsultują się z nimi i wymieniają się z nimi informacjami na temat zagrożeń i incydentów mających wpływ na ich sieci i systemy informatyczne;

ib) opracowują, we współpracy z ENISA, wytyczne dotyczące kryteriów dla danego sektora w odniesieniu do zgłaszania znaczących incydentów oprócz parametrów określonych w art. 14 ust. 2 w celu wspólnej wykładni, spójnego stosowania i harmonijnego wdrażania w Unii. **[Popr. 78]**

3a. Sieć współpracy publikuje raz w roku sprawozdanie za poprzednie 12 miesięcy oparte na działalności sieci i na sprawozdaniu podsumowującym przekazanym zgodnie z art. 14 ust. 4 niniejszej dyrektywy. **[Popr. 79]**

4. Komisja ustanawia – w drodze aktów wykonawczych – niezbędne środki w celu ułatwienia współpracy ~~pomiędzy właściwymi organami i Komisją~~, o której mowa w ust. 2 i 3***, pomiędzy pojedynczymi punktami kontaktowymi, Komisją i ENISA***. Te akty wykonawcze przyjmuje się zgodnie z procedurą ~~doradczą~~ ***sprawdzającą***, o której mowa w art. 19 ust. 2. **[Popr. 80]**

Artykuł 9

Bezpieczny system wymiany informacji

1. Wymiana szczególnie chronionych i poufnych informacji w ramach sieci współpracy odbywa się za pośrednictwem bezpiecznej infrastruktury.

1a. Uczestnicy bezpiecznej infrastruktury spełniają m.in. odpowiednie wymogi poufności i bezpieczeństwa zgodnie z dyrektywą 95/46/WE i rozporządzeniem (WE) nr 45/2001 na każdym etapie przetwarzania. **[Popr. 81]**

~~2. Komisja jest uprawniona do przyjęcia aktów delegowanych zgodnie z art. 18 dotyczących określenia kryteriów, jakie państwo członkowskie musi spełnić, aby móc uczestniczyć w bezpiecznym systemie wymiany informacji, w odniesieniu do:~~

~~a) dostępności bezpiecznej i odpornej infrastruktury komunikacyjnej i informacyjnej na poziomie krajowym, kompatybilnej i interoperacyjnej z bezpieczną infrastrukturą sieci współpracy, zgodnie z art. 7 ust. 3, oraz~~

~~b) zapewnienia właściwemu organowi i CERT odpowiednich zasobów i procedur technicznych i finansowych oraz zasobów ludzkich w celu umożliwienia im skutecznego, efektywnego i bezpiecznego uczestnictwa w bezpiecznym systemie wymiany informacji zgodnie z art. 6 ust. 3, art. 7 ust. 2 i art. 7 ust. 3.~~ **[Popr. 82]**

3. Komisja przyjmuje – w drodze aktów ~~wykonawczych – decyzje dotyczące dostępu państw członkowskich do tej bezpiecznej infrastruktury, zgodnie z kryteriami, o~~ ***delegowanych, zgodnie z art. 18 – wspólny zestaw norm w zakresie wzajemnych połączeń i bezpieczeństwa, do*** których ~~mowa w ust. 2 i 3. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 19 ust. 3~~***pojedyncze punkty kontaktowe mają się stosować przed wymianą szczególnie chronionych i poufnych informacji w ramach sieci współpracy.*** **[Popr. 83]**

Artykuł 10

Wczesne ostrzeżenia

1. W ramach sieci współpracy ~~właściwe organy~~ ***pojedyncze punkty kontaktowe*** lub Komisja wydają wczesne ostrzeżenia dotyczące zagrożeń i incydentów, które spełniają co najmniej jeden z następujących warunków:

~~a) ich skala szybko rośnie lub może szybko wzrosnąć;~~

b) ~~przekraczają one lub mogą przekroczyć~~ ***w ocenie pojedynczego punktu kontaktowego dane zagrożenie lub incydent potencjalnie przekracza*** krajowe zdolności reagowania;

c) ~~mają one~~***w ocenie pojedynczego punktu kontaktowego lub Komisji dane zagrożenie lub incydent ma*** wpływ ~~lub mogą mieć wpływ~~ na więcej niż jedno państwo członkowskie. **[Popr. 84]**

2. Wraz z wczesnym ostrzeżeniem ~~właściwe organy~~ ***pojedyncze punkty kontaktowe*** i Komisja przekazują ***bez zbędnej zwłoki*** wszelkie stosowne informacje będące w ich posiadaniu, które mogą być przydatne do oceny zagrożenia lub incydentu. **[Popr. 85]**

~~3. Na wniosek państwa członkowskiego lub z własnej inicjatywy Komisja może zwrócić się do państwa członkowskiego o przedstawienie istotnych informacji dotyczących określonego zagrożenia lub incydentu.~~ **[Popr. 86]**

4. W sytuacji gdy zachodzi podejrzenie, iż zagrożenie lub incydent będące przedmiotem wczesnego ostrzeżenia ~~mają charakter przestępczy, właściwe organy lub Komisja powiadamiają~~ ***noszą znamiona poważnego przestępstwa, oraz jeżeli odnośny podmiot gospodarczy zgłosił incydenty noszące znamiona poważnego przestępstwa, zgodnie z art. 15 ust. 4, państwa członkowskie dopilnowują, aby – w stosownych przypadkach – poinformowano o tym*** działające przy Europolu Europejskie Centrum ds. Walki z Cyberprzestępczością. **[Popr. 87]**

4a. Członkowie sieci współpracy nie podają do wiadomości publicznej żadnych otrzymanych informacji na temat zagrożeń i incydentów, o których mowa w ust. 1, bez otrzymania uprzednio zgody pojedynczego punktu kontaktowego dokonującego zgłoszenia.

Ponadto przed wymianą informacji w ramach sieci współpracy dokonujący zgłoszenia pojedynczy punkt kontaktowy informuje o swoim zamiarze podmiot gospodarczy, którego dane informacje dotyczą, i dokonuje ich anonimizacji, jeżeli podmiot gospodarczy uzna to za stosowne. **[Popr. 88]**

4b. W sytuacji gdy zachodzi podejrzenie, iż zagrożenie lub incydent będące przedmiotem wczesnego ostrzeżenia stanowią poważne zagrożenie lub poważny incydent o charakterze technicznym transnarodowym, pojedyncze punkty kontaktowe lub Komisja powiadamiają ENISA. **[Popr. 89]**

5. Komisja jest uprawniona do przyjęcia aktów delegowanych zgodnie z art. 18, dotyczących sprecyzowania zagrożeń i incydentów prowadzących do wczesnych ostrzeżeń, o których mowa w ust. 1 niniejszego artykułu.

Artykuł 11

Skoordynowana reakcja

1. Po otrzymaniu wczesnego ostrzeżenia, o którym mowa w art. 10, ~~właściwe organy~~ ***pojedyncze punkty kontaktowe*** – po przeanalizowaniu właściwych informacji – uzgadniają ***bez zbędnej zwłoki*** skoordynowaną reakcję zgodnie z unijnym planem współpracy w zakresie bezpieczeństwa sieci i informacji, o którym mowa w art. 12. **[Popr. 90]**

2. Informacje o różnych środkach przyjętych na poziomie krajowym w wyniku skoordynowanej reakcji przekazuje się do sieci współpracy.

Artykuł 12

Unijny plan współpracy w zakresie bezpieczeństwa sieci i informacji

1. Komisja jest uprawniona do przyjęcia, w drodze aktów wykonawczych, unijnego planu współpracy w zakresie bezpieczeństwa sieci i informacji. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 19 ust. 3.

2. Unijny plan współpracy w zakresie bezpieczeństwa sieci i informacji obejmuje:

a) do celów art. 10:

określenie formatu i procedur gromadzenia i wymiany kompatybilnych i porównywalnych informacji na temat zagrożeń i incydentów przez ~~właściwe organy~~ ***pojedyncze punkty kontaktowe***; **[Popr. 91]**

określenie procedur i kryteriów oceny zagrożeń i incydentów przez sieć współpracy;

b) procedury, jakie należy stosować w przypadku skoordynowanych reakcji na mocy art. 11, w tym określenie funkcji i obowiązków oraz procedur współpracy;

c) plan działania dotyczący ćwiczeń i szkoleń w zakresie bezpieczeństwa sieci i informacji, mający na celu wzmocnienie, zatwierdzenie i sprawdzenie głównego planu;

d) program dotyczący transferu wiedzy między państwami członkowskimi w odniesieniu do budowy zdolności i wzajemnego uczenia się;

e) program dotyczący działań informacyjnych i szkoleń między państwami członkowskimi.

3. Unijny plan współpracy w zakresie bezpieczeństwa sieci i informacji przyjmuje się nie później niż jeden rok po wejściu w życie niniejszej dyrektywy i regularnie poddaje się go przeglądowi. ***Wyniki każdego przeglądu są przekazywane Parlamentowi Europejskiemu.*** **[Popr. 92]**

3a. Należy zagwarantować spójność między unijnym planem współpracy w zakresie bezpieczeństwa sieci i informacji a krajowymi strategiami w zakresie bezpieczeństwa sieci i informacji i krajowymi planami współpracy w zakresie bezpieczeństwa sieci i informacji zgodnie z art. 5. **[Popr. 93]**

Artykuł 13

Współpraca międzynarodowa

Bez uszczerbku dla możliwości podejmowania nieformalnej współpracy międzynarodowej przez sieć współpracy, Unia może zawierać umowy międzynarodowe z państwami trzecimi lub organizacjami międzynarodowymi, umożliwiając oraz organizując ich udział w określonych działaniach sieci współpracy. Takie umowy uwzględniają potrzebę zapewnienia odpowiedniej ochrony danych osobowych~~, które są przekazywane~~ ***przekazywanych*** w ramach sieci współpracy ***i określają procedurę monitorowania, którą należy stosować, aby zagwarantować ochronę takich danych osobowych. Parlament Europejski jest informowany o negocjacjach w sprawie tych umów. Każde przekazanie danych osobowych odbiorcom z siedzibą w krajach poza Unią odbywa się z zgodnie z art. 25 i 26 dyrektywy 95/46/WE oraz z art. 9 rozporządzenia (WE) nr 45/2001***. **[Popr. 94]**

Artykuł 13a

Poziom krytyczności podmiotów gospodarczych

Państwa członkowskie mogą określić poziom krytyczności podmiotów gospodarczych, biorąc pod uwagę specyfikę sektorów, parametry obejmujące znaczenie konkretnego podmiotu gospodarczego dla utrzymania wystarczającego poziomu usług sektorowych, liczbę części dostarczanych przez dany podmiot gospodarczy oraz okres, po którego upływie brak ciągłości świadczenia usług podstawowych przez podmiot gospodarczy ma negatywny wpływ na utrzymanie kluczowych działań gospodarczych i społecznych. **[Popr. 95]**

ROZDZIAŁ IV

BEZPIECZEŃSTWO SIECI I SYSTEMÓW INFORMATYCZNYCH ORGANÓW ADMINISTRACJI PUBLICZNEJ I PODMIOTÓW GOSPODARCZYCH

Artykuł 14

Wymogi w zakresie bezpieczeństwa i zgłaszanie incydentów

1. Państwa członkowskie zapewniają zastosowanie przez ~~organy administracji publicznej i~~ podmioty gospodarcze właściwych ***i proporcjonalnych*** środków technicznych i organizacyjnych w celu ~~przeciwdziałania zagrożeniom~~ ***wykrywania zagrożeń***, na jakie narażone są kontrolowane i wykorzystywane przez nie sieci i systemy informatyczne***, oraz skutecznego przeciwdziałania im***. ~~Uwzględniając aktualny stan~~ ***Środki te gwarantują poziom bezpieczeństwa proporcjonalny do istniejącego ryzyka z uwzględnieniem aktualnego stanu*** wiedzy i technologii~~, środki te zapewniają poziom bezpieczeństwa stosowny do istniejącego zagrożenia~~. W szczególności należy ~~podjąć~~ ***przyjąć*** środki zapobiegające incydentom ~~dotyczącym~~ ***mającym wpływ na bezpieczeństwo ich*** sieci i systemów informatycznych ~~organów administracji publicznej i podmiotów gospodarczych~~ oraz minimalizujące wpływ tych incydentów na świadczone przez nie podstawowe usługi, zapewniając tym samym ciągłość usług opartych na tych sieciach i systemach informatycznych. **[Popr. 96]**

2. Państwa członkowskie dopilnowują, aby o~~rgany administracji publicznej oraz~~ podmioty gospodarcze ***niezwłocznie*** zgłaszały ~~właściwym organom~~ ***właściwemu organowi lub pojedynczemu punktowi kontaktowemu*** incydenty mające znaczące konsekwencje dla ~~bezpieczeństwa~~ ***ciągłości*** świadczonych przez nie usług podstawowych. ***Zgłoszenie nie może narażać strony zgłaszającej na większą odpowiedzialność.***

Aby określić znaczenie konsekwencji danego incydentu, uwzględnia się m.in. następujące parametry: **[Popr. 97]**

a) liczbę użytkowników korzystających z usługi podstawowej, na którą ma wpływ dany incydent; **[Popr. 98]**

b) czas trwania incydentu; **[Popr. 99]**

c) zasięg geograficzny związany z obszarem, którego dotyczy incydent. **[Popr. 100]**

Parametry te zostają doprecyzowane zgodnie z art. 8 ust. 3 lit. ib). **[Popr. 101]**

2a. Podmioty gospodarcze zgłaszają incydenty, o których mowa w ust. 1 i 2, właściwemu organowi lub pojedynczemu punktowi kontaktowemu w państwie członkowskim, w którym incydent ma wpływ na podstawową usługę. Jeżeli incydent ma wpływ na usługi podstawowe w więcej niż jednym państwie członkowskim, pojedynczy punkt kontaktowy, który otrzymał zgłoszenie, alarmuje pozostałe zainteresowane pojedyncze punkty kontaktowe, opierając się na informacjach dostarczonych przez dany podmiot gospodarczy. Podmiotowi gospodarczemu przekazuje się w możliwie najkrótszym terminie informacje na temat innych pojedynczych punktów kontaktowych powiadomionych o incydencie, a także wszelkich podjętych kroków, rezultatów oraz wszelkie inne informacje mające znaczenie dla incydentu. **[Popr. 102]**

2b. Jeżeli zgłoszenie zawiera dane osobowe, jest ono ujawniane wyłącznie odbiorcom powiadomionego właściwego organu lub pojedynczego punktu kontaktowego, którzy muszą przetwarzać te dane w ramach swoich obowiązków zgodnie z przepisami dotyczącymi ochrony danych. Zakres ujawnianych danych ogranicza się do tego, co niezbędne do wykonywania tych zadań. **[Popr. 103]**

2c. Podmioty gospodarcze nieobjęte załącznikiem II mogą zgłaszać incydenty określone w art. 14 ust. 2 na zasadzie dobrowolności. **[Popr. 104]**

3. Ust. 1 i 2 stosuje się do wszystkich podmiotów gospodarczych świadczących usługi w obrębie Unii Europejskiej.

4. ~~W przypadku gdy właściwy organ uznaje,~~ ***Po konsultacji z powiadomionym właściwym organem i zainteresowanym podmiotem gospodarczym pojedynczy punkt kontaktowy może poinformować opinię publiczną o pojedynczych incydentach, jeżeli uzna,*** że ~~ujawnienie incydentu leży w interesie publicznym, może on podać informację o incydencie do wiadomości publicznej lub zobowiązać do tego organy administracji publicznej lub podmioty gospodarcze.~~ ***wiedza obywateli na ten temat jest niezbędna, by zapobiec incydentowi bądź uporać się z bieżącym incydentem, lub jeżeli podmiot gospodarczy, którego dotyczy incydent, odmówił niezwłocznego usunięcia poważnej strukturalnej usterki związanej z tym incydentem***.

Przed podaniem informacji o incydencie do wiadomości publicznej powiadomiony właściwy organ dopilnowuje, aby zainteresowany podmiot gospodarczy miał możliwość wypowiedzenia się oraz aby decyzja o upublicznieniu takich informacji była należycie wyważona w odniesieniu do interesu publicznego.

W przypadku podania informacji o pojedynczych incydentach do wiadomości publicznej powiadomiony właściwy organ lub pojedynczy punkt kontaktowy dopilnowuje, aby odbyło się to jak najbardziej anonimowo.

Właściwy organ lub pojedynczy punkt kontaktowy udziela, w miarę możliwości, zainteresowanemu podmiotowi gospodarczemu informacji pomocnych w skutecznym rozwiązaniu zgłoszonego incydentu.

Raz do roku ~~właściwy organ~~ ***pojedynczy punkt kontaktowy*** przekazuje sieci współpracy sprawozdanie podsumowujące otrzymane zgłoszenia ~~i działania~~ ***, w tym informacje o liczbie zgłoszeń i parametrach incydentu wyszczególnionych w ust. 2 niniejszego artykułu, oraz działania*** podjęte zgodnie z niniejszym ustępem. **[Popr. 105]**

4a. Państwa członkowskie powinny zachęcać podmioty gospodarcze, aby na zasadzie dobrowolności informowały opinię publiczną w swoich sprawozdaniach finansowych o incydentach związanych ze swoją działalnością. **[Popr. 106]**

~~5. Komisja jest uprawniona do przyjęcia aktów delegowanych zgodnie z art. 18 dotyczących określenia okoliczności, w których organy administracji publicznej i podmioty gospodarcze są zobowiązane do zgłaszania incydentów.~~ **[Popr. 107]**

6. ~~Z zastrzeżeniem wszelkich aktów delegowanych przyjętych na mocy ust. 5,~~ Właściwe organy ***lub pojedyncze punkty kontaktowe*** mogą przyjąć wytyczne~~, a w razie konieczności wydać instrukcje~~ dotyczące okoliczności, w których ~~organy administracji publicznej i~~ podmioty gospodarcze są zobowiązane do zgłaszania incydentów. **[Popr. 108]**

7. Komisja jest uprawniona do określenia – w drodze aktów wykonawczych – formatów i procedur mających zastosowanie do celów ust. 2. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 19 ust. 3.

8. Ustępów 1 i 2 nie stosuje się w odniesieniu do mikroprzedsiębiorstw określonych w zaleceniu Komisji 2003/361/WE ([1])***, chyba że mikroprzedsiębiorstwo działa jako jednostka zależna podmiotu gospodarczego, o którym mowa w art. 3 pkt 8 lit. b)***. **[Popr. 109]**

8a. Państwa członkowskie mogą podjąć decyzję o stosowaniu do organów administracji publicznej odpowiednio niniejszego artykułu i art. 15. **[Popr. 110]**

Artykuł 15

Wdrażanie i egzekwowanie

1. Państwa członkowskie zapewniają właściwym organom ~~wszelkie~~ ***i pojedynczym punktom kontaktowym*** uprawnienia niezbędne do ~~badania przypadków niewypełniania przez organy administracji publicznej lub podmioty gospodarcze zobowiązań ciążących~~ ***zapewnienia zgodności ze zobowiązaniami ciążącymi*** na nich na mocy art. 14 oraz ich wpływu na bezpieczeństwo sieci i systemów informatycznych. **[Popr. 111]**

([1]) Zalecenie Komisji 2003/361/WE z dnia 6 maja 2003 r. w sprawie definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz.U. L 124 z 20.5.2003, s. 36).

2. Państwa członkowskie zapewniają właściwym organom ***i pojedynczym punktom kontaktowym*** uprawnienia, na podstawie których mogą one wymagać od podmiotów gospodarczych ~~i organów administracji publicznej~~: **[Popr. 112]**

a) przekazywania informacji potrzebnych do oceny bezpieczeństwa ich sieci i systemów informatycznych, w tym dokumentów dotyczących polityki w zakresie bezpieczeństwa;

b) ~~poddania się audytowi~~ ***dostarczenia dowodów skutecznej realizacji polityki w zakresie*** bezpieczeństwa ~~przeprowadzonemu~~ ***, takich jak wyniki audytu bezpieczeństwa przeprowadzonego*** przez wykwalifikowany niezależny podmiot lub organ krajowy, oraz udostępnienia ~~wyników tego audytu~~ ***tych dowodów*** właściwemu organowi ***lub pojedynczemu punktowi kontaktowemu***. **[Popr. 113]**

Kierując taki wniosek, właściwe organy i pojedyncze punkty kontaktowe podają cel wniosku i określają dokładnie, jakie informacje są wymagane. **[Popr. 114]**

3. Państwa członkowskie zapewniają właściwym organom ***i pojedynczym punktom kontaktowym*** uprawnienia do wydawania wiążących instrukcji dla podmiotów gospodarczych ~~i organów administracji publicznej~~. **[Popr. 115]**

3a. W drodze odstępstwa od ust. 2 lit. b) niniejszego artykułu państwa członkowskie mogą zdecydować, że właściwe organy lub pojedyncze punkty kontaktowe, w zależności od wymogów, mają stosować inną procedurę w odniesieniu do konkretnych podmiotów gospodarczych w oparciu o ich poziom krytyczności określony zgodnie z art. 13a. W przypadku gdy państwa członkowskie podejmą taką decyzję:

a) właściwe organy lub pojedyncze punkty kontaktowe, w zależności od wymogów, są uprawnione do wystąpienia z wystarczająco konkretnym wnioskiem do podmiotów gospodarczych zobowiązującym je do dostarczenia dowodów skutecznej realizacji polityki w zakresie bezpieczeństwa, takich jak wyniki audytu bezpieczeństwa przeprowadzonego przez wykwalifikowanego audytora wewnętrznego, oraz udostępnienia tych dowodów właściwemu organowi lub pojedynczemu punktowi kontaktowemu;

b) w stosownych przypadkach właściwy organ lub pojedynczy punkt kontaktowy mogą – po przedłożeniu przez podmiot gospodarczy dokumentów, o których mowa w lit. a) – zażądać dodatkowych dowodów lub przeprowadzenia dodatkowego audytu przez wykwalifikowany niezależny podmiot lub organ krajowy.

3b. Państwa członkowskie mogą podjąć decyzję o zmniejszeniu liczby i intensywności audytów w odniesieniu do danego podmiotu gospodarczego, jeśli przeprowadzony w nim audyt bezpieczeństwa wykazał konsekwentną zgodność z postanowieniami rozdziału IV. **[Popr. 116]**

4. Właściwe organy ~~zgłaszają~~ ***i pojedyncze punkty kontaktowe informują zainteresowane podmioty gospodarcze o możliwości zgłaszania*** organom ścigania ~~poważne incydenty, które mogą mieć charakter przestępczy~~ ***incydentów noszących znamiona poważnego przestępstwa***. **[Popr. 117]**

5. ***Bez uszczerbku dla obowiązującego prawa o ochronie danych,*** w przypadku incydentów prowadzących do ~~naruszeń~~ ***naruszenia przepisów o ochronie*** danych osobowych właściwe organy ***i pojedyncze punkty kontaktowe*** działają w ścisłej współpracy z organami ochrony danych osobowych. ***Pojedyncze punkty kontaktowe i organy ochrony danych opracowują we współpracy z ENISA mechanizmy wymiany informacji oraz jednolity wzór formularza wykorzystywanego zarówno w przypadku zgłoszeń na podstawie art. 14 ust. 2 niniejszej dyrektywy, jak i na podstawie prawa Unii o ochronie danych.*** **[Popr. 118]**

6. Państwa członkowskie zapewniają możliwość poddania kontroli sądowej wszelkich obowiązków nałożonych na ~~organy administracji publicznej oraz~~ podmioty gospodarcze na mocy niniejszego rozdziału. **[Popr. 119]**

6a. Państwa członkowskie mogą podjąć decyzję o stosowaniu odpowiednio art. 14 i niniejszego artykułu do organów administracji publicznej. **[Popr. 120]**

Artykuł 16

Normalizacja

1. W celu zapewnienia spójnego wdrażania art. 14 ust. 1 państwa członkowskie***, nie nakazując stosowania żadnej konkretnej technologii,*** wspierają stosowanie ***europejskich lub międzynarodowych interoperacyjnych*** norm lub specyfikacji mających znaczenie dla bezpieczeństwa sieci i informacji. **[Popr. 121]**

2. Komisja ~~sporządza w drodze aktów wykonawczych wykaz~~ ***nadaje odpowiedniemu organowi normalizacji europejskiej mandat do sporządzenia, w konsultacji z odpowiednimi zainteresowanymi stronami, wykazu*** norm ***lub specyfikacji***, o których mowa w ust. 1. Wykaz ten zostaje opublikowany w *Dzienniku Urzędowym Unii Europejskiej*. **[Popr. 122]**

ROZDZIAŁ V

PRZEPISY KOŃCOWE

Artykuł 17

Sankcje

1. Państwa członkowskie ustanawiają przepisy o sankcjach mających zastosowanie, gdy naruszone zostaną krajowe przepisy przyjęte na podstawie niniejszej dyrektywy, i stosują wszelkie niezbędne środki, aby zapewnić ich wykonanie. Przewidziane sankcje muszą być skuteczne, proporcjonalne i odstraszające. Najpóźniej w dniu, w którym przypada termin transpozycji niniejszej dyrektywy, państwa członkowskie powiadamiają Komisję o tych przepisach, a następnie niezwłocznie powiadamiają ją o wszelkich zmianach mających wpływ na te przepisy.

1a. Państwa członkowskie zapewniają, że sankcje, o których mowa w ust. 1 niniejszego artykułu, mają zastosowanie wyłącznie w przypadku, gdy podmiot gospodarczy celowo lub w wyniku rażącego zaniedbania nie wywiązał się z obowiązków przewidzianych w rozdziale IV. **[Popr. 123]**

2. Państwa członkowskie dopilnowują, by w przypadku incydentów zagrażających bezpieczeństwu danych osobowych przewidziane sankcje były zgodne z sankcjami przewidzianymi w rozporządzeniu Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych ([1]).

Artykuł 18

Wykonywanie przekazanych uprawnień

1. Powierzenie Komisji uprawnień do przyjęcia aktów delegowanych podlega warunkom określonym w niniejszym artykule.

2. Uprawnienia do przyjęcia aktów delegowanych, o których mowa w art. 9 ust. 3, i art. 10 ust. 5 ~~i art. 14 ust. 5~~, powierza się Komisji. Komisja sporządza sprawozdanie dotyczące przekazania uprawnień nie później niż dziewięć miesięcy przed końcem okresu wynoszącego pięć lat. Przekazanie uprawnień zostaje automatycznie przedłużone na takie same okresy, chyba że Parlament Europejski lub Rada sprzeciwią się takiemu przedłużeniu nie później niż trzy miesiące przed końcem każdego okresu.

3. Przekazanie ~~uprawnień~~ ***uprawnienia***, o którym mowa w art. 9 ust. 3 i art. 10 ust. 5 ~~i art. 14 ust. 5,~~ może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna od następnego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej lub w określonym w tej decyzji późniejszym terminie. Nie wpływa ona na ważność jakichkolwiek już obowiązujących aktów delegowanych. **[Popr. 124]**

4. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.

([1]) SEC(2012) 72 final.

5. Akt delegowany przyjęty na podstawie art. 9 ust. 3 i art. 10 ust. 5 ~~i art. 14 ust. 5~~ wchodzi w życie tylko ~~wówczas, gdy~~ ***wtedy***, ***kiedy*** Parlament Europejski albo Rada nie wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie, lub ~~gdy~~ ***kiedy***, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady. **[Popr. 125]**

Artykuł 19

Procedura komitetowa

1. Komisję wspomaga komitet (Komitet ds. Bezpieczeństwa Sieci i Informacji). Komitet jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.

2. W przypadku odesłania do niniejszego ustępu stosuje się art. 4 rozporządzenia (UE) nr 182/2011.

3. W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011.

Artykuł 20

Przegląd

Komisja dokonuje okresowego przeglądu funkcjonowania niniejszej dyrektywy***, w szczególności wykazu zawartego w załączniku II,*** i składa Parlamentowi Europejskiemu i Radzie sprawozdania na ten temat. Pierwsze sprawozdanie należy przedłożyć nie później niż trzy lata po dacie transpozycji, o której mowa w art. 21. W tym celu Komisja może zwrócić się do państw członkowskich o bezzwłoczne dostarczenie informacji. **[Popr. 126]**

Artykuł 21

Transpozycja

1. Państwa członkowskie przyjmują i publikują, najpóźniej do dnia [półtora roku po przyjęciu] r., przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania niniejszej dyrektywy. Niezwłocznie przekazują Komisji tekst tych przepisów.

Państwa członkowskie stosują te przepisy od dnia [półtora roku po przyjęciu] r.

Przepisy przyjęte przez państwa członkowskie zawierają odniesienie do niniejszej dyrektywy lub odniesienie takie towarzyszy ich urzędowej publikacji. Metody dokonywania takiego odniesienia określane są przez państwa członkowskie.

2. Państwa członkowskie przekazują Komisji tekst podstawowych przepisów prawa krajowego, przyjętych w dziedzinie objętej niniejszą dyrektywą.

Artykuł 22

Wejście w życie

Niniejsza dyrektywa wchodzi w życie [dwudziestego] dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Artykuł 23

Adresaci

Niniejsza dyrektywa skierowana jest do państw członkowskich.

Sporządzono w

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodniczący	*Przewodniczący*

ZAŁĄCZNIK I

~~Zespoły~~ ***Wymogi i zadania zespołów*** reagowania na incydenty komputerowe (CERT) ~~– wymogi i zadania~~ **[Popr. 127]**

Wymogi i zadania dla CERT są odpowiednio i jasno określone i umocowane w strategiach lub regulacjach krajowych. Obejmują one następujące elementy:

(1) Wymogi dotyczące CERT

a) CERT ~~zapewnia~~ ***zapewniają*** wysoką dostępność swoich usług łączności poprzez unikanie pojedynczych punktów awarii oraz ~~dysponuje~~ ***dysponują*** różnymi kanałami, za pomocą których ***zawsze*** można się z ~~nim~~ ***nimi*** skontaktować i za pomocą których ~~on sam może~~ ***one same mogą*** się kontaktować z innymi. Ponadto kanały komunikacyjne są wyraźnie określone i dobrze znane wśród użytkowników CERT i wśród współpracujących partnerów. **[Popr. 128]**

b) CERT wdraża środki mające na celu zapewnienie poufności, integralności, dostępności i wiarygodności otrzymywanych i przetwarzanych informacji, oraz zarządza tymi środkami.

c) Biura CERT oraz wspierające systemy informatyczne są zlokalizowane w bezpiecznych miejscach z ***zabezpieczonymi sieciowymi systemami informatycznymi***. **[Popr. 129]**

d) W celu monitorowania działalności CERT i zapewnienia jej ciągłej poprawy należy utworzyć system zarządzania jakością usług. System ten jest oparty na jasno zdefiniowanych metodach pomiaru, które obejmują formalne poziomy usług oraz kluczowe wskaźniki wyników.

e) Ciągłość działania:

— CERT musi być wyposażony w odpowiedni system zarządzania i dysponowania wnioskami w celu ułatwienia ich późniejszego przekazywania.

— CERT dysponuje wystarczającą liczbą personelu, aby zapewnić nieprzerwaną dostępność usług.

— CERT korzysta z infrastruktury o gwarantowanej ciągłości działania. W tym kontekście należy zapewnić CERT systemy redundantne oraz rezerwowy lokal w celu zapewnienia stałego dostępu do środków komunikacji.

(2) Zadania CERT

a) Zadania CERT obejmują co najmniej:

— ***wykrywanie i*** monitorowanie incydentów na poziomie krajowym; **[Popr. 130]**

— przekazywanie zainteresowanym stronom wczesnych ostrzeżeń, ogłaszanie alarmów, wydawanie ogłoszeń i przekazywanie informacji skierowanych do zainteresowanych stron i dotyczących zagrożeń oraz incydentów;

— reagowanie na incydenty;

— zapewnianie dynamicznej analizy zagrożeń i incydentów oraz zintegrowanej oceny sytuacji;

— informowanie opinii publicznej o zagrożeniach związanych z działalnością online,

— ***czynny udział w unijnych i międzynarodowych sieciach współpracy CERT;*** **[Popr. 131]**

— organizowanie kampanii w zakresie bezpieczeństwa sieci i informacji.

b) CERT nawiązuje współpracę z sektorem prywatnym.

c) W celu ułatwienia współpracy CERT wspiera przyjmowanie i wykorzystywanie wspólnych lub znormalizowanych praktyk w odniesieniu do:

— procedur postępowania w przypadku wystąpienia incydentów i zagrożeń;

— systemów klasyfikacji incydentów, zagrożeń i informacji;

— taksonomii metod pomiarów;

— formatów wymiany informacji dotyczących zagrożeń i incydentów oraz konwencji nazewnictwa systemów.

ZAŁĄCZNIK II

Wykaz podmiotów gospodarczych

~~o których mowa w art. 3 ust. 8 lit. a):~~

~~1. platformy handlu elektronicznego~~

~~2. internetowe portale płatnicze~~

~~3. portale społecznościowe~~

~~4. wyszukiwarki~~

~~5. usługi chmur obliczeniowych~~

~~6. sklepy z aplikacjami~~

~~o których mowa w art. 3 ust. 8 lit. b):~~ **[Popr. 132]**

1. Energetyka

a) Energia elektryczna

dostawcy ~~energii elektrycznej i gazu~~

operatorzy systemów dystrybucyjnych ~~energii elektrycznej lub gazu~~ oraz detaliści sprzedający energię elektryczną ~~lub gaz~~ konsumentom końcowym

~~operatorzy systemów przesyłowych gazu ziemnego, operatorzy systemu magazynowania i operatorzy systemów LNG~~

operatorzy systemów przesyłowych energii elektrycznej

b) Ropa naftowa

podmioty eksploatujące rurociągi przesyłowe i magazyny ropy naftowej

— ***operatorzy instalacji służących do produkcji, rafinacji, przetwarzania, magazynowania i przesyłu ropy naftowej***

c) Gaz

~~podmioty działające na rynku gazu i energii elektrycznej~~

dostawcy

— ***operatorzy systemów dystrybucyjnych oraz detaliści sprzedający gaz konsumentom końcowym***

— ***operatorzy systemów przesyłowych gazu ziemnego, operatorzy systemu magazynowania i operatorzy systemów LNG***

— operatorzy instalacji służących do produkcji ~~ropy naftowej i~~ ***, rafinacji, przetwarzania, magazynowania i przesyłu*** gazu ziemnego~~, obiekty służące do rafinacji i przetwarzania~~

— ***podmioty działające na rynku gazu*** *[Popr. 133]*

2. Transport

~~przewoźnicy lotniczy (przewozy pasażerskie i towarowe)~~

~~przewoźnicy morscy (przedsiębiorstwa świadczące usługi pasażerskiego transportu morskiego i przybrzeżnego oraz przedsiębiorstwa świadczące usługi towarowego transportu morskiego i przybrzeżnego)~~

~~koleje (zarządcy infrastruktury, przedsiębiorstwa zintegrowane oraz przedsiębiorstwa transportu kolejowego)~~

~~porty lotnicze~~

~~porty~~

~~operatorzy zarządzający ruchem~~

~~pomocnicze usługi logistyczne: a) magazynowanie oraz składowanie, b) przeładunek i c) pozostała działalność wspomagająca transport~~

a) Transport drogowy

(i) operatorzy zarządzający ruchem

(ii) pomocnicze usługi logistyczne:

— magazynowanie i składowanie

— przeładunek oraz

— pozostała działalność wspomagająca transport

b) Transport kolejowy

(i) koleje (zarządcy infrastruktury, przedsiębiorstwa zintegrowane oraz przedsiębiorstwa transportu kolejowego)

(ii) operatorzy zarządzający ruchem

(iii) pomocnicze usługi logistyczne:

— magazynowanie i składowanie

— przeładunek oraz

— pozostała działalność wspomagająca transport

c) Transport lotniczy

(i) przewoźnicy lotniczy (przewozy pasażerskie i towarowe)

(ii) porty lotnicze

(iii) operatorzy zarządzający ruchem

(iv) pomocnicze usługi logistyczne:

— magazynowanie

— przeładunek oraz

— pozostała działalność wspomagająca transport

d) Transport morski

(i) przewoźnicy morscy (przedsiębiorstwa świadczące usługi pasażerskiego transportu śródlądowego, morskiego i przybrzeżnego oraz przedsiębiorstwa świadczące usługi towarowego transportu śródlądowego, morskiego i przybrzeżnego) *[Popr. 134]*

3. Bankowość: instytucje kredytowe zgodnie z art. 4 pkt 1 dyrektywy Parlamentu Europejskiego i Rady 2006/48/WE ([1]).

([1]) Dyrektywa Parlamentu Europejskiego i Rady 2006/48/WE z dnia 14 czerwca 2006 r. w sprawie podejmowania i prowadzenia działalności przez instytucje kredytowe (Dz.U. L 177 z 30.6.2006, s. 1).

4. ~~Infrastruktura rynków finansowych: giełdy papierów wartościowych i izby rozliczeniowe partnerów centralnych~~ ***Infrastruktura rynków finansowych: rynki regulowane, wielostronne platformy obrotu, zorganizowane platformy obrotu i izby rozliczeniowe kontrahentów centralnych*** **[Popr. 135]**

5. Służba zdrowia: punkty opieki zdrowotnej (w tym szpitale i prywatne kliniki) i inne podmioty świadczące usługi opieki zdrowotnej

5a. Produkcja wody i zaopatrzenie w wodę **[Popr. 136]**

5b. Łańcuch dostaw żywności **[Popr. 137]**

5c. Internetowe punkty wymiany **[Popr. 138]**