Parlament Europejski
2019-2024

Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych

2022/0085(COD)

1.3.2023

OPINIA

Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych

dla Komisji Przemysłu, Badań Naukowych i Energii

w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii (COM(2022)0122 – C9-0122/2022 – 2022/0085(COD))

Sprawozdawca komisji opiniodawczej (*): Tomas Tobé

(*) Zaangażowana komisja – art. 57 Regulaminu

PA_Legam

POPRAWKI

Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych zwraca się do Komisji Przemysłu, Badań Naukowych i Energii, jako komisji przedmiotowo właściwej, o wzięcie pod uwagę następujących poprawek:

Poprawka 1

Wniosek dotyczący rozporządzenia
Motyw 4

Tekst proponowany przez Komisję	*Poprawka*
(4) Instytucje, organy i agencje Unii stanowią atrakcyjne cele i muszą stawiać czoła wysoko wykwalifikowanym i dobrze zaopatrzonym agresorom, a także innym zagrożeniom. Jednocześnie poziom i dojrzałość w zakresie cyberodporności oraz zdolność do wykrywania szkodliwych działań w cyberprzestrzeni i reagowania na nie znacznie się w tych podmiotach różnią. Dla funkcjonowania administracji unijnej konieczne jest zatem, aby instytucje, organy i agencje Unii osiągnęły wysoki wspólny poziom cyberbezpieczeństwa dzięki podstawowemu poziomowi cyberbezpieczeństwa (minimalnemu zbiorowi przepisów dotyczących cyberbezpieczeństwa, z którymi muszą być zgodne sieci i systemy informatyczne oraz których muszą przestrzegać ich operatorzy i użytkownicy, aby zminimalizować ryzyko w cyberprzestrzeni) oraz dzięki wymianie informacji i współpracy.	(4) Instytucje, organy i agencje Unii ***stanowiły i*** stanowią atrakcyjne cele i muszą stawiać czoła wysoko wykwalifikowanym i dobrze zaopatrzonym agresorom, a także innym zagrożeniom. Jednocześnie poziom i dojrzałość w zakresie cyberodporności oraz zdolność do wykrywania szkodliwych działań w cyberprzestrzeni i reagowania na nie znacznie się w tych podmiotach różnią. Dla funkcjonowania administracji unijnej konieczne jest zatem, aby instytucje, organy i agencje Unii osiągnęły wysoki wspólny poziom cyberbezpieczeństwa dzięki podstawowemu poziomowi cyberbezpieczeństwa (minimalnemu zbiorowi przepisów dotyczących cyberbezpieczeństwa, z którymi muszą być zgodne sieci i systemy informatyczne oraz których muszą przestrzegać ich operatorzy i użytkownicy, aby zminimalizować ryzyko w cyberprzestrzeni) oraz dzięki wymianie informacji i współpracy.

Poprawka 2

Wniosek dotyczący rozporządzenia
Motyw 5

Tekst proponowany przez Komisję	*Poprawka*
(5) Dyrektywa [wniosek dotyczący dyrektywy NIS 2] w sprawie środków na	(5) Dyrektywa [wniosek dotyczący dyrektywy NIS 2] w sprawie środków na

rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii ma na celu dalszą poprawę odporności podmiotów publicznych i prywatnych, właściwych organów i instytucji krajowych, jak również całej Unii pod względem cyberbezpieczeństwa oraz dalsze zwiększenie ich zdolności reagowania na incydenty w zakresie cyberbezpieczeństwa. Należy zatem zadbać o to, by podobnymi środkami objęto instytucje, organy i agencje Unii, poprzez ustanowienie przepisów, które są zgodne z dyrektywą [wniosek dotyczący dyrektywy NIS 2] i odzwierciedlają przewidziany w niej poziom ambicji.	rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii ma na celu dalszą poprawę odporności podmiotów publicznych i prywatnych, właściwych organów i instytucji krajowych, jak również całej Unii pod względem cyberbezpieczeństwa oraz dalsze zwiększenie ich zdolności reagowania na incydenty w zakresie cyberbezpieczeństwa. Należy zatem zadbać o to, by podobnymi środkami objęto instytucje, organy i agencje Unii, poprzez ustanowienie przepisów, które są zgodne z dyrektywą [wniosek dotyczący dyrektywy NIS 2] i odzwierciedlają przewidziany w niej poziom ambicji. ***Wymogi bezpieczeństwa powinny być co najmniej równe minimalnym wymogom bezpieczeństwa podmiotów określonym w dyrektywie (UE) 2022/2555 lub od nich wyższe.***

Poprawka 3

Wniosek dotyczący rozporządzenia
Motyw 6 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(6a) Należy zapewnić instytucjom, organom, urzędom i agencjom Unii odpowiednie środki i narzędzia, by wzmocnić ich cyberodporność. W związku z tym należy wprowadzić odpowiednie mechanizmy koordynacji, które usprawnią i zwiększą efektywność procesów decyzyjnych.

Poprawka 4

Wniosek dotyczący rozporządzenia
Motyw 22

Tekst proponowany przez Komisję	*Poprawka*
(22) Wszelkie dane osobowe	(22) Wszelkie dane osobowe

przetwarzane na podstawie niniejszego rozporządzenia należy przetwarzać zgodnie z przepisami o ochronie danych, w tym z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2018/1725[7].

przetwarzane na podstawie niniejszego rozporządzenia należy przetwarzać zgodnie z przepisami ***Unii*** o ochronie danych, w tym z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2018/1725[7]. ***Niniejsze rozporządzenie nie ma wpływu na stosowanie przepisów Unii regulujących przetwarzanie danych osobowych, włącznie z zadaniami i kompetencjami EIOD. CERT-UE i IICB powinny ściśle współpracować z EIOD i pracownikami specjalizującymi się w ochronie danych w instytucjach, organach, urzędach i agencjach Unii, aby zapewnić pełną zgodność z unijnym prawem o ochronie danych.***

[7] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39).

[7] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39).

Poprawka 5

Wniosek dotyczący rozporządzenia
Motyw 22 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(22a) Systemy i usługi cyberbezpieczeństwa związane z zapobieganiem cyberzagrożeniom, ich wykrywaniem i reagowaniem na nie powinny być zgodne z prawem ochrony danych i prawem dotyczącym prywatności oraz obejmować odpowiednie zabezpieczenia techniczne i organizacyjne, aby zapewnić taką zgodność w odpowiedzialny sposób.

Poprawka 6

Wniosek dotyczący rozporządzenia
Motyw 23

Tekst proponowany przez Komisję	*Poprawka*
(23) Postępowanie z informacjami przez CERT-UE oraz instytucje, organy i agencje Unii powinno być zgodne z przepisami określonymi w rozporządzeniu [rozporządzenie w sprawie bezpieczeństwa informacji będące przedmiotem wniosku]. W celu zapewnienia koordynacji w sprawach bezpieczeństwa o wszelkich kontaktach z CERT-UE, które inicjują lub do których dążą krajowe służby bezpieczeństwa i wywiadu, należy bezzwłocznie informować Dyrekcję Komisji ds. Bezpieczeństwa oraz przewodniczącego IICB.	(23) Postępowanie z informacjami przez CERT-UE oraz instytucje, organy i agencje Unii powinno być zgodne z ***unijnymi*** przepisami ***dotyczącymi bezpieczeństwa informacji, w szczególności*** określonymi w rozporządzeniu [rozporządzenie w sprawie bezpieczeństwa informacji będące przedmiotem wniosku]. W celu zapewnienia koordynacji w sprawach bezpieczeństwa o wszelkich kontaktach z CERT-UE, które inicjują lub do których dążą krajowe służby bezpieczeństwa i wywiadu, należy bezzwłocznie informować Dyrekcję Komisji ds. Bezpieczeństwa oraz przewodniczącego IICB.

Poprawka 7

Wniosek dotyczący rozporządzenia
Motyw 25 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(25a) Zgodnie z art. 42 ust. 1 rozporządzenia (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię 17 maja 2022 r.,

Poprawka 8

Wniosek dotyczący rozporządzenia
Artykuł 4 – ustęp 5

Tekst proponowany przez Komisję	*Poprawka*
5. Każda instytucja, każdy organ	5. Każda instytucja, każdy organ

i każda agencja Unii wyznaczają lokalnego urzędnika ds. cyberbezpieczeństwa lub osobę pełniącą równoważną funkcję, która działa jako pojedynczy punkt kontaktowy w odniesieniu do wszystkich kwestii związanych z cyberbezpieczeństwem.	i każda agencja Unii wyznaczają lokalnego urzędnika ds. cyberbezpieczeństwa lub osobę pełniącą równoważną funkcję, która działa jako pojedynczy punkt kontaktowy w odniesieniu do wszystkich kwestii związanych z cyberbezpieczeństwem. ***Lokalny urzędnik ds. cyberbezpieczeństwa współpracuje z inspektorem ochrony danych wyznaczonym zgodnie z art. 43 rozporządzenia (UE) 2018/1725 przy rozwiązywaniu problemów dotyczących pokrywających się działań, takich jak stosowanie zasady ochrony danych już w fazie projektowania i domyślnej ochrony danych w odniesieniu do środków cyberbezpieczeństwa oraz wybór środków cyberbezpieczeństwa obejmujących ochronę danych osobowych, zintegrowane zarządzanie ryzykiem i zintegrowane postępowanie w przypadku cyberincydentów.***

Poprawka 9

Wniosek dotyczący rozporządzenia
Artykuł 9 – ustęp 3 – akapit 1 – litera k a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	ka) Europejskiego Inspektora Ochrony Danych;

Poprawka 10

Wniosek dotyczący rozporządzenia
Artykuł 9 – ustęp 3 – akapit 1 – litera k b (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	kb) Agencję Unii Europejskiej ds. Współpracy Organów Ścigania.

Poprawka 11

Wniosek dotyczący rozporządzenia
Artykuł 12 – ustęp 2 – litera e a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	ea) informuje Europejskiego Inspektora Ochrony Danych o wszelkich przesłankach wskazujących na naruszenie przez instytucję, organ, urząd lub agencję Unii obowiązków określonych w niniejszym rozporządzeniu; obejmuje to niezgodne z prawem przetwarzanie danych osobowych;

Poprawka 12

Wniosek dotyczący rozporządzenia
Artykuł 12 – ustęp 2 – litera e b (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	eb) ściśle współpracuje z Europejskim Inspektorem Ochrony Danych przy reagowaniu na incydenty, których skutkiem są naruszenia ochrony danych osobowych lub naruszenia poufności łączności elektronicznej.

Poprawka 13

Wniosek dotyczący rozporządzenia
Artykuł 12 – ustęp 7 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	7a. CERT-UE informuje Europejskiego Inspektora Ochrony Danych, gdy reaguje na istotne podatności, znaczące incydenty lub poważne ataki, które mogą doprowadzić do naruszeń ochrony danych osobowych lub naruszeń poufności łączności elektronicznej.

Poprawka 14

Wniosek dotyczący rozporządzenia
Artykuł 18 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. Przepisy rozporządzenia (WE) nr 1049/2001 Parlamentu Europejskiego i Rady[9] mają zastosowanie w odniesieniu do wniosków o udzielenie publicznego dostępu do dokumentów przechowywanych przez CERT-UE, w tym wynikającego z tego rozporządzenia obowiązku konsultowania się z innymi instytucjami, organami i agencjami Unii, jeśli przedmiotem wniosku są ich dokumenty.	2. Przepisy rozporządzenia (WE) nr 1049/2001 Parlamentu Europejskiego i Rady[9] mają zastosowanie w odniesieniu do wniosków o udzielenie publicznego dostępu do dokumentów przechowywanych przez CERT-UE, w tym wynikającego z tego rozporządzenia obowiązku konsultowania się z innymi instytucjami, organami i agencjami Unii ***lub w stosownych przypadkach państwami członkowskimi***, jeśli przedmiotem wniosku są ich dokumenty.
[9] 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).	[9] 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).

Poprawka 15

Wniosek dotyczący rozporządzenia
Artykuł 18 – ustęp 3 – akapit 1 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	Wszelkie przetwarzanie, wymiana, gromadzenie lub zatrzymywanie danych osobowych przez CERT-UE, IICB oraz instytucje, organy, urzędy i agencje Unii ogranicza się do przetwarzania, wymiany, gromadzenia lub zatrzymywania, które jest absolutnie niezbędne i prowadzone wyłącznie w celu wypełnienia ich odpowiednich obowiązków wynikających z niniejszego rozporządzenia.

Poprawka 16

Wniosek dotyczący rozporządzenia
Artykuł 18 – ustęp 3 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	3a. Do dnia [1 rok po dacie wejścia w życie niniejszego rozporządzenia] Komisja przyjmuje akt delegowany, aby sprecyzować, jakie działania w zakresie przetwarzania danych osobowych są dozwolone na mocy niniejszego rozporządzenia, w tym cel przetwarzania, kategorie danych osobowych, kategorie osób, których dane dotyczą, warunki przetwarzania danych, maksymalne okresy zatrzymywania, definicję administratorów danych i podmiotów przetwarzających dane oraz odbiorców w przypadku przekazywania danych.
	Akt delegowany, o którym mowa w akapicie pierwszym, ogranicza czynności przetwarzania do tych, które są absolutnie niezbędne, i wymaga, aby były one jak najbardziej ukierunkowane i nie obejmowały niezróżnicowanego zatrzymywania danych o ruchu lub treściach.
	Komisja zmienia akt delegowany, o którym mowa w akapicie pierwszym, gdy stwierdzi istotne zmiany dotyczące konieczności, konkretnych celów lub podmiotów uczestniczących w przetwarzaniu danych osobowych do celów niniejszego rozporządzenia.

Poprawka 17

Wniosek dotyczący rozporządzenia
Artykuł 18 – ustęp 4

Tekst proponowany przez Komisję	*Poprawka*
4. CERT-UE oraz korzystające z jego usług instytucje, organy i agencje Unii postępują z informacjami w sposób zgodny z przepisami określonymi w [wniosek	4. CERT-UE oraz korzystające z jego usług instytucje, organy i agencje Unii postępują z informacjami w sposób zgodny z ***unijnymi*** przepisami ***dotyczącymi***

dotyczący rozporządzenia w sprawie bezpieczeństwa informacji].	***bezpieczeństwa informacji, w szczególności*** określonymi w [wniosek dotyczący rozporządzenia w sprawie bezpieczeństwa informacji].

Poprawka 18

Wniosek dotyczący rozporządzenia
Artykuł 18 – ustęp 5

Tekst proponowany przez Komisję	*Poprawka*
5. O wszelkich kontaktach z CERT-UE, które inicjują lub do których dążą krajowe służby bezpieczeństwa i wywiadu, bezzwłocznie informuje się Dyrekcję Komisji ds. Bezpieczeństwa oraz przewodniczącego IICB.	5. O wszelkich kontaktach z CERT-UE, które inicjują lub do których dążą krajowe służby bezpieczeństwa i wywiadu, bezzwłocznie informuje się Dyrekcję Komisji ds. Bezpieczeństwa***, Europol*** oraz przewodniczącego IICB.

Poprawka 19

Wniosek dotyczący rozporządzenia
Artykuł 19 – nagłówek

Tekst proponowany przez Komisję	*Poprawka*
Obowiązki w zakresie wymiany informacji	Wymiana informacji

Poprawka 20

Wniosek dotyczący rozporządzenia
Artykuł 19 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Aby ***umożliwić CERT-UE koordynację*** zarządzania podatnościami oraz reagowania na incydenty, ***CERT-UE może zwracać się do instytucji, organów i agencji Unii o przekazanie mu informacji*** z ich odpowiednich rejestrów zasobów ***informatycznych***, które to informacje są istotne ***z punktu widzenia wsparcia świadczonego przez CERT-UE. Instytucja, organ lub agencja***, do ***których***	1. Aby ***CERT-UE mógł wykonywać zadania określone w art. 12, w szczególności w celu koordynacji*** zarządzania podatnościami oraz reagowania na incydenty, ***instytucje, organy lub agencje Unii – na wniosek CERT-UE – przekazują CERT-UE informacje*** z ich odpowiednich rejestrów zasobów ***ICT***, które to informacje są istotne ***dla CERT-UE, w tym informacje o***

się zwrócono, bez zbędnej zwłoki ***przekazują*** przedmiotowe informacje oraz ich wszelkie późniejsze aktualizacje.	***wszelkich zmianach w ich otoczeniu informatycznym. Podmiot***, do ***którego*** się zwrócono, bez zbędnej zwłoki ***przekazuje*** przedmiotowe informacje oraz ich wszelkie późniejsze aktualizacje. ***Bez uszczerbku dla rozporządzenia (UE) 2018/1725 każda wymiana danych między CERT-UE a instytucjami, organami, urzędami lub agencjami Unii odbywa się zgodnie z zasadami jasnych gwarancji dotyczących określonych przypadków użycia oraz z zastosowaniem traktatów o wzajemnej pomocy prawnej i innych umów, aby zapewnić wysoki poziom ochrony praw podczas rozpatrywania wniosków o transgraniczny dostęp do danych.***

Poprawka 21

Wniosek dotyczący rozporządzenia
Artykuł 19 – ustęp 1 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	1a. Instytucje, organy, urzędy i agencje Unii mogą dobrowolnie przekazywać CERT-UE informacje na temat zagrożeń cyberbezpieczeństwa, incydentów, zdarzeń potencjalnie wypadkowych i podatności, które ich dotyczą. Mogą też zwrócić się do CERT-UE o dalszą pomoc techniczną i doradztwo w celu zwalczania cyberincydentów i poważnych ataków. CERT-UE może rozpatrywać zgłoszenia obowiązkowe przed zgłoszeniami dobrowolnymi, z wyjątkiem przypadków należycie uzasadnionych i pilnych dobrowolnych wniosków instytucji, organów, urzędów i agencji Unii.

Poprawka 22

Wniosek dotyczący rozporządzenia
Artykuł 19 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. CERT-UE może prowadzić wymianę informacji dotyczących konkretnych incydentów, które to informacje umożliwiają identyfikację instytucji, organu lub agencji Unii dotkniętych incydentem, wyłącznie za ***zgodą*** tego podmiotu. CERT-UE może prowadzić wymianę informacji dotyczących konkretnych incydentów, które to informacje umożliwiają identyfikację celu, w który wymierzony jest cyberincydent, wyłącznie za ***zgodą*** podmiotu dotkniętego incydentem.	3. CERT-UE może prowadzić wymianę informacji dotyczących konkretnych incydentów, które to informacje umożliwiają identyfikację instytucji, organu lub agencji Unii dotkniętych incydentem, wyłącznie za ***zezwoleniem*** tego podmiotu. CERT-UE może prowadzić wymianę informacji dotyczących konkretnych incydentów, które to informacje umożliwiają identyfikację celu, w który wymierzony jest cyberincydent, wyłącznie za ***zezwoleniem*** podmiotu dotkniętego incydentem. ***Jeżeli jest to konieczne do wykonywania powierzonych mu zadań, CERT-UE może wymieniać informacje dotyczące konkretnego incydentu, w tym w przypadku braku zezwolenia instytucji, organu, urzędu lub agencji Unii, dotkniętych incydentem. O każdej takiej wymianie informacji powiadamia się z wyprzedzeniem instytucję, organ, urząd lub agencję Unii.***

Poprawka 23

Wniosek dotyczący rozporządzenia
Artykuł 19 – ustęp 4

Tekst proponowany przez Komisję	*Poprawka*
4. Obowiązki w zakresie wymiany informacji nie obejmują informacji niejawnych UE (EUCI) ani informacji, które służby bezpieczeństwa lub wywiadu lub organy ścigania państwa członkowskiego przekazały instytucji, organowi lub agencji Unii ***z wyraźnym zastrzeżeniem,*** że ***nie można ich udostępniać*** CERT-UE.	4. Obowiązki w zakresie wymiany informacji nie obejmują informacji niejawnych UE (EUCI) ani informacji, które służby bezpieczeństwa lub wywiadu lub organy ścigania państwa członkowskiego przekazały instytucji, organowi lub agencji Unii***, chyba*** że ***służby lub organy te zezwolą na udostępnienie tych informacji*** CERT-UE.

Poprawka 24

Wniosek dotyczący rozporządzenia
Artykuł 20 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. CERT-UE co miesiąc przekazuje ENISA sprawozdanie podsumowujące zawierające zanonimizowane i zagregowane dane dotyczące znaczących cyberzagrożeń, znaczących podatności i znaczących incydentów zgłoszonych zgodnie z ust. 1.	3. CERT-UE co miesiąc przekazuje ENISA sprawozdanie podsumowujące zawierające zanonimizowane i zagregowane dane dotyczące znaczących cyberzagrożeń, znaczących podatności i znaczących incydentów zgłoszonych zgodnie z ust. 1. ***Sprawozdanie to podaje się do wiadomości publicznej, z zastrzeżeniem odpowiednich przepisów Unii dotyczących bezpieczeństwa informacji, w szczególności określonych w [proponowanym rozporządzeniu w sprawie bezpieczeństwa informacji].***

Poprawka 25

Wniosek dotyczący rozporządzenia
Artykuł 20 – ustęp 5

Tekst proponowany przez Komisję	*Poprawka*
5. Obowiązki w zakresie zgłaszania nie obejmują EUCI ani informacji, które służby bezpieczeństwa i wywiadu lub organy ścigania państwa członkowskiego przekazały instytucji, organowi lub agencji Unii ***z wyraźnym zastrzeżeniem,*** że ***nie można ich udostępniać*** CERT-UE.	5. Obowiązki w zakresie zgłaszania nie obejmują EUCI ani informacji, które służby bezpieczeństwa i wywiadu lub organy ścigania państwa członkowskiego przekazały instytucji, organowi lub agencji Unii***, chyba*** że ***służby lub organy te zezwolą na udostępnienie tych informacji*** CERT-UE.

Poprawka 26

Wniosek dotyczący rozporządzenia
Artykuł 21 – ustęp 4

Tekst proponowany przez Komisję	*Poprawka*
4. IICB wydaje wytyczne dotyczące koordynacji reakcji na incydenty	4. IICB wydaje wytyczne dotyczące koordynacji reakcji na incydenty

i współpracy w tym zakresie w odniesieniu do znaczących incydentów. W przypadku podejrzenia, że incydent nosi znamiona przestępstwa, CERT-UE ***doradza, jak zgłaszać*** incydent organom ścigania.	i współpracy w tym zakresie w odniesieniu do znaczących incydentów. W przypadku podejrzenia, że incydent nosi znamiona przestępstwa, CERT-UE ***lub IICB bez zbędnej zwłoki zgłasza*** incydent organom ścigania.

Poprawka 27

Wniosek dotyczący rozporządzenia
Artykuł 24 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	Artykuł 24a
	Wykonywanie przekazanych uprawnień
	1. Powierzenie Komisji uprawnień do przyjmowania aktów delegowanych podlega warunkom określonym w niniejszym artykule.
	2. Uprawnienia do przyjmowania aktów delegowanych, o których mowa w art. 18 ust. 3a, powierza się Komisji na czas nieokreślony od dnia [jeden dzień po dacie wejścia w życie niniejszego rozporządzenia].
	3. Przekazanie uprawnień, o którym mowa w art. 18 ust. 3a, 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 następnego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej lub w późniejszym terminie określonym w tej decyzji. Nie wpływa ona na ważność już obowiązujących aktów delegowanych.
	4. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.
	5. Akt delegowany przyjęty na podstawie art. 18 ust. 3a wchodzi w życie

	tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie, lub gdy, 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.

Poprawka 28

Wniosek dotyczący rozporządzenia
Załącznik II – akapit 1 – punkt 2 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	2a) wykorzystywanie szyfrowania w trakcie przechowywania, szyfrowania w trakcie przesyłania i szyfrowania end-to-end, gdy jest to możliwe;

PROCEDURA W KOMISJI OPINIODAWCZEJ

Tytuł	Ustanowienie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii
Odsyłacze	COM(2022)0122 – C9-0122/2022 – 2022/0085(COD)
Komisja przedmiotowo właściwa Data ogłoszenia na posiedzeniu	ITRE 4.4.2022
Opinia wydana przez Data ogłoszenia na posiedzeniu	LIBE 4.4.2022
Zaangażowane komisje - Data ogłoszenia na posiedzeniu	15.9.2022
Sprawozdawca komisji opiniodawczej Data powołania	Tomas Tobé 12.12.2022
Rozpatrzenie w komisji	31.1.2023
Data przyjęcia	1.3.2023
Wynik głosowania końcowego	+: 62 –: 0 0: 1
Posłowie obecni podczas głosowania końcowego	Magdalena Adamowicz, Abir Al-Sahlani, Malik Azmani, Katarina Barley, Pietro Bartolo, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Karolin Braunsberger-Reinhold, Patrick Breyer, Saskia Bricmont, Patricia Chagnon, Caterina Chinnici, Clare Daly, Lena Düpont, Lucia Ďuriš Nicholsonová, Maria Grapini, Sylvie Guillaume, Andrzej Halicki, Evin Incir, Sophia in ‘t Veld, Patryk Jaki, Marina Kaljurand, Assita Kanko, Fabienne Keller, Łukasz Kohut, Moritz Körner, Alice Kuhnke, Jeroen Lenaers, Juan Fernando López Aguilar, Erik Marquardt, Nuno Melo, Maite Pagazaurtundúa, Karlo Ressler, Diana Riba i Giner, Birgit Sippel, Sara Skyttedal, Vincenzo Sofo, Tineke Strik, Ramona Strugariu, Annalisa Tardino, Tomas Tobé, Yana Toom, Milan Uhrík, Tom Vandendriessche, Jadwiga Wiśniewska
Zastępcy obecni podczas głosowania końcowego	Susanna Ceccardi, Gwendoline Delbos-Corfield, Loucas Fourlas, Beata Kempa, Philippe Olivier, Dragoş Tudorache, Petar Vitanov, Tomáš Zdechovský
Zastępcy (art. 209 ust. 7) obecni podczas głosowania końcowego	Gheorghe Falcă, Jean-François Jalkh, Petra Kammerevert, Marisa Matias, Martina Michels, Ljudmila Novak, Stanislav Polčák, Mick Wallace, Bernhard Zimniok

GŁOSOWANIE KOŃCOWE W FORMIE GŁOSOWANIA IMIENNEGO W KOMISJI OPINIODAWCZEJ

62	+
ECR	Patryk Jaki, Assita Kanko, Beata Kempa, Vincenzo Sofo, Jadwiga Wiśniewska
ID	Susanna Ceccardi, Patricia Chagnon, Jean-François Jalkh, Philippe Olivier, Annalisa Tardino, Tom Vandendriessche, Bernhard Zimniok
PPE	Magdalena Adamowicz, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Karolin Braunsberger-Reinhold, Lena Düpont, Gheorghe Falcă, Loucas Fourlas, Andrzej Halicki, Jeroen Lenaers, Nuno Melo, Ljudmila Novak, Stanislav Polčák, Karlo Ressler, Sara Skyttedal, Tomas Tobé, Tomáš Zdechovský
Renew	Abir Al-Sahlani, Malik Azmani, Lucia Ďuriš Nicholsonová, Sophia in 't Veld, Fabienne Keller, Moritz Körner, Maite Pagazaurtundúa, Ramona Strugariu, Yana Toom, Dragoş Tudorache
S&D	Katarina Barley, Pietro Bartolo, Caterina Chinnici, Maria Grapini, Sylvie Guillaume, Evin Incir, Marina Kaljurand, Petra Kammerevert, Łukasz Kohut, Juan Fernando López Aguilar, Birgit Sippel, Petar Vitanov
The Left	Clare Daly, Marisa Matias, Martina Michels, Mick Wallace
Verts/ALE	Patrick Breyer, Saskia Bricmont, Gwendoline Delbos-Corfield, Alice Kuhnke, Erik Marquardt, Diana Riba i Giner, Tineke Strik

0	-

1	0
NI	Milan Uhrík

Objaśnienie używanych znaków:
+ : za
- : przeciw
0 : wstrzymało się