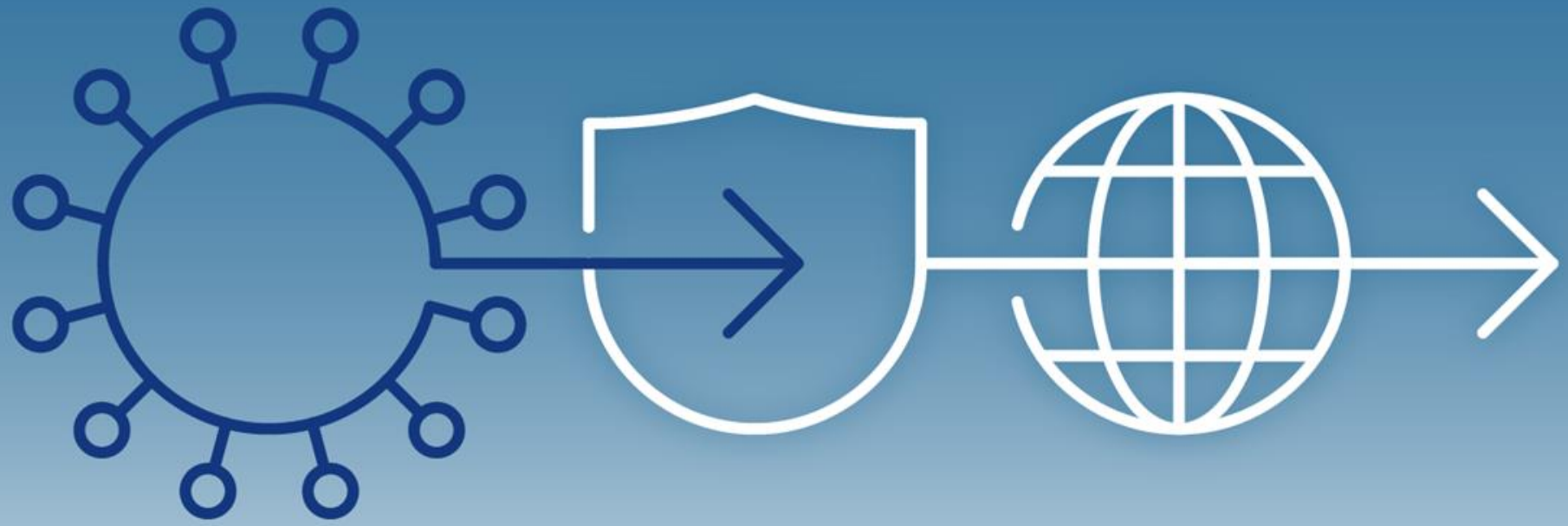
Konferencja Naukowa Bezpieczeństwo w Internecie – Cyberpandemia

22-23 października 2020 r.



NCBC

Sektorowa Rada ds. Kompetencji
Telekomunikacja i Cyberbezpieczeństwo

UNIWERSYTET KARDYNAŁA STEFANA WYSZYŃSKIEGO W WARSZAWIE

PTI
POLSKIE TOWARZYSTWO INFORMATYCZNE

Naukowe Centrum Prawno-informatyczne

Ochrona danych osobowych w systemie cyberbezpieczeństwa

dr Beata Konieczna-Drzewiecka

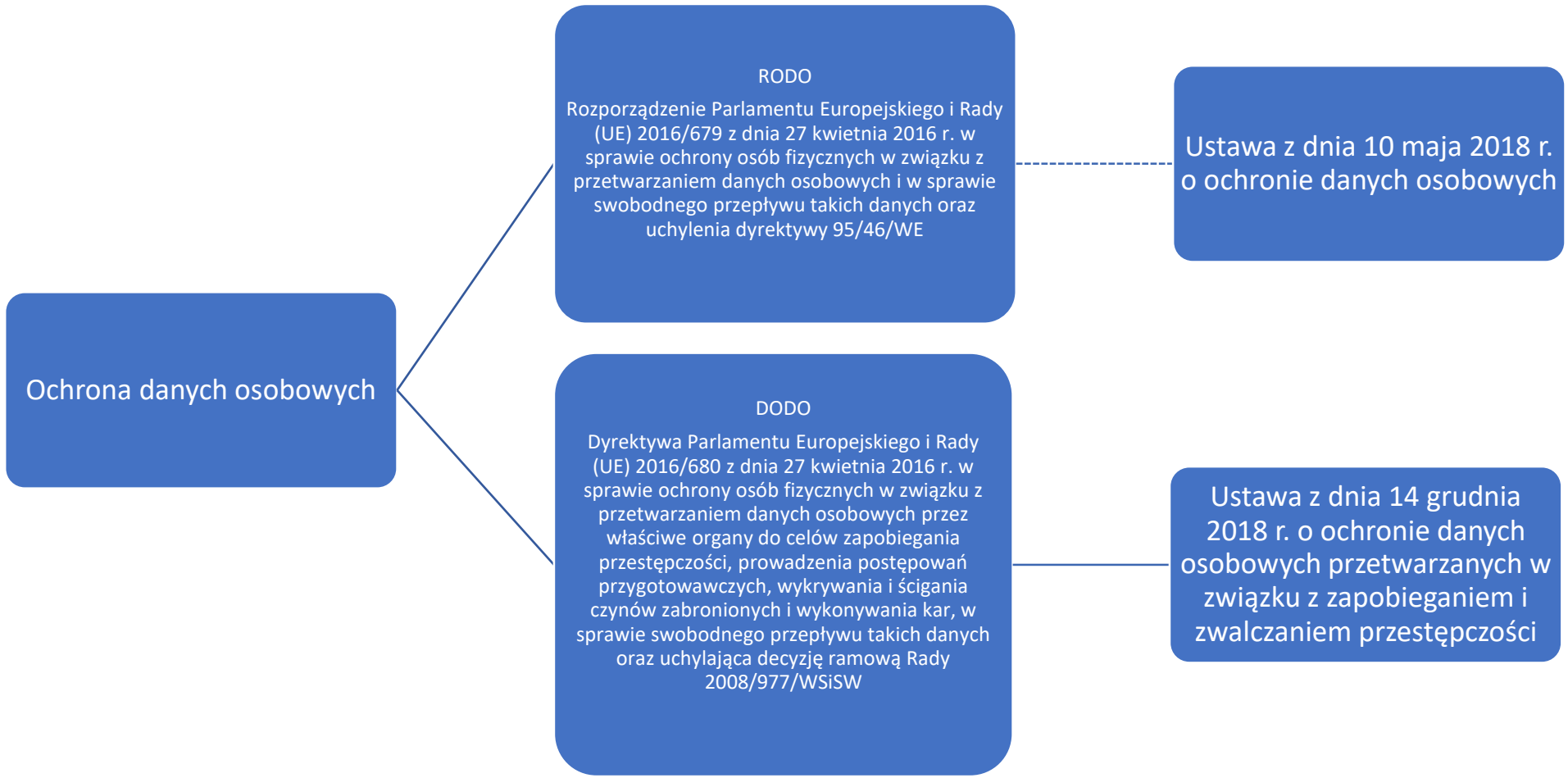
Piotr Drobek

Unia Europejska

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (**RODO**)

Dyrektywa Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa 2016/1148), tzw. **Dyrektywa NIS**

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013, tzw. **Akt o cyberbezpieczeństwie**

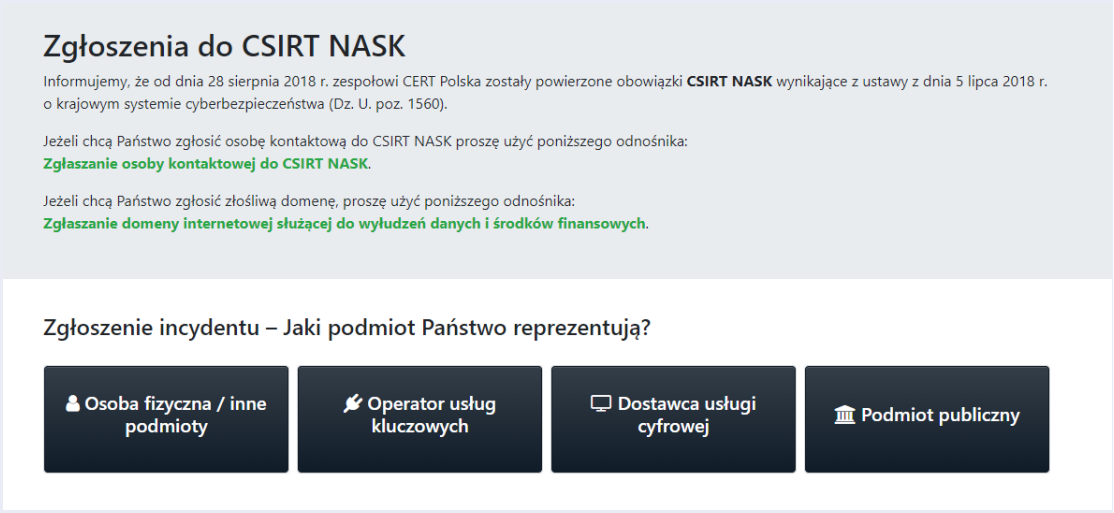

Ochrona danych osobowych
RODO
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych
DODO
Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW
Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości

Ustawa z 5.07.2018r. o krajowym systemie cyberbezpieczeństwa Dz.U. 2018 poz. 1560

Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej

Uchwała Nr 125 Rady Ministrów z dnia 22.10.2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, M.P. z 2019 r. poz. 1037

RODO	CyberBezpU
RODO nie określa szczegółowych wymogów bezpieczeństwa. Wskazówki co do tego, jak wdrożyć odpowiednie środki oraz wykazać przestrzeganie prawa przez administratora lub podmiot przetwarzający dane – w szczególności jeżeli chodzi o identyfikowanie ryzyka związanego z przetwarzaniem, o jego ocenę pod kątem źródła, charakteru, prawdopodobieństwa i wagi oraz o najlepsze praktyki pozwalające zminimalizować to ryzyko - mogą być przekazane **w szczególności w formie** zatwierdzonych kodeksów postępowania, **zatwierdzonych mechanizmów certyfikacji**	Operatorzy Usług Kluczowych są zobowiązani do wdrożenia dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej zgodnej z wymaganiami norm PN-EN ISO/IEC 27001 i PN-EE ISO 22301 oraz szacowania ryzyka związanego z cyberbezpieczeństwem i wdrażania adekwatnych zabezpieczeń.
	Rozporządzenie w sprawie ENISA – RAMY CERTYFIKACJI CYBERBEZPIECZEŃSTWA art. 46 Europejskie ramy certyfikacji cyberbezpieczeństwa. art. 47 Unijny kroczący program prac na rzecz europejskich programów certyfikacji cyberbezpieczeństwa. art. 57. Krajowe programy certyfikacji cyberbezpieczeństwa i krajowe certyfikaty cyberbezpieczeństwa. art. 58. Krajowe organy ds. certyfikacji cyberbezpieczeństwa. art 62. Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa.

RODO	CyberBezpU
W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.	Istotnym obowiązkiem Operatorów Usług Kluczowych jest również wdrożenie procesu zarządzania incydentami, przekazywanie **w ciągu 24 godzin** informacji o poważnych incydentach i ich obsługa we współpracy z jednym z trzech CSIRT (Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego).
Zgłoszenia można dokonać na 4 sposoby: Elektronicznie poprzez wypełnienie **dedykowanego formularza elektronicznego** dostępnego bezpośrednio na platformie biznes.gov.pl będącego odwzorowaniem formularza dostępnego w załączniku. Elektronicznie poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePUAP: **/UODO/SkrytkaESP** Elektronicznie poprzez wysłanie wypełnionego formularza (dostępnego poniżej w załączniku) za pomocą **pisma ogólnego dostępnego na platformie biznes.gov.pl** (Jak znaleźć Urząd w formularzu pisma ogólnego?) lub **platformie epuap.gov.pl** Tradycyjną pocztą wysyłając wypełniony formularz na adres Urzędu.	

Zgłoszenie incydentu – Jaki podmiot Państwo reprezentują?

- **Osoba fizyczna / inne podmioty**
- **Operator usług kluczowych**
- **Dostawca usługi cyfrowej**
- **Podmiot publiczny**

Prosimy o wybranie odpowiedniej kategorii:

- **Podejrzana wiadomość e-mail/SMS**
  Podejrzane załączniki/SMSy, phishing, szantaż
- **$ Oszustwo**
  Fałszywe sklepy internetowe i inne próby podszywania się
- **Złośliwe oprogramowanie**
  Próbki wirusów lub pliki zaszyfrowane ransomware
- **Podatności**
  Błędy w oprogramowaniu lub aplikacjach internetowych
- **Nielegalne treści**
  Zgłoszenia przeznaczone dla zespołu Dyżurnet.pl
- **Inne**
  Wszystkie inne incydenty niepasujące do poprzednich kategorii

Zgłoszenie incydentu – Jaki podmiot Państwo reprezentują?

Osoba fizyczna / inne podmioty | **Operator usług kluczowych** | Dostawca usługi cyfrowej | Podmiot publiczny

Czy reprezentują Państwo podmiot z listy operatorów usług kluczowych i chcą Państwo dokonać zgłoszenia incydentu poważnego?

Operatorem usługi kluczowej jest podmiot, o którym mowa w załączniku nr 1 do ustawy, posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, wobec którego organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu za operatora usługi kluczowej. Sektory, podsektory oraz rodzaje podmiotów określa załącznik nr 1 do ustawy.

Progi **uznania incydentu za poważny** zależą od liczby użytkowników dotkniętych incydentem, czasu oddziaływania incydentu na świadczoną usługę oraz zasięgu geograficznego incydentu. Kryteria dla poszczególnych sektorów określone są przez Radę Ministrów w drodze rozporządzenia.

Zgłoszenie incydentu za pomocą formularza dostępnego po wybraniu opcji "Tak" **stanowi wypełnienie obowiązku** wynikającego z art 11 ust 1 pkt 4 ustawy z dnia 5 lipca 2018 (Dz. U. poz. 1560) o krajowym systemie cyberbezpieczeństwa.

Tak
Reprezentuję operatora usług kluczowych i chcę zgłosić incydent poważny.

Nie
Chcę zgłosić incydent nieklasyfikowany jako poważny zgodnie z powyższą definicją.

Sektorowa Rada ds. Kompetencji
Telekomunikacja i Cyberbezpieczeństwo

UNIWERSYTET KARDYNAŁA STEFANA WYSZYŃSKIEGO W WARSZAWIE

POLSKIE TOWARZYSTWO INFORMATYCZNE

Naukowe Centrum Prawno-informatyczne

Osoba fizyczna / inne podmioty | Operator usług kluczowych | **Dostawca usługi cyfrowej** | Podmiot publiczny

Czy reprezentują Państwo dostawcę usługi cyfrowej i chcą Państwo dokonać zgłoszenia incydentu istotnego?

Dostawcą usługi cyfrowej jest osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej mająca siedzibę lub zarząd na terytorium Rzeczypospolitej Polskiej albo przedstawiciela mającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, świadcząca usługę cyfrową, z wyjątkiem mikroprzedsiębiorców i małych przedsiębiorców, o których mowa w art. 7 ust. 1 pkt 1 i 2 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. poz. 646 i 1479). Rodzaje usług cyfrowych określa załącznik nr 2 do ustawy z dnia 5 lipca 2018 o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560).

Jako **incydent istotny** określa sie incydent, który ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 rozporządzenia wykonawczego Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiającego zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz. Urz. UE L 26 z 31.01.2018, str. 48), zwanego dalej „rozporządzeniem wykonawczym 2018/151";

Zgłoszenie incydentu za pomocą formularza dostępnego po wybraniu opcji "Tak" **stanowi wypełnienie obowiązku** wynikającego z art 18 ust 1 pkt 4 ustawy z dnia 5 lipca 2018 (Dz. U. poz. 1560) o krajowym systemie cyberbezpieczeństwa.

Tak
Reprezentuję dostawcę usługi cyfrowej i chcę zgłosić incydent istotny.

Nie
Chcę zgłosić incydent nieklasyfikowany jako istotny zgodnie z powyższą definicją.

Zgłoszenie incydentu – Jaki podmiot Państwo reprezentują?

Osoba fizyczna / inne podmioty | Operator usług kluczowych | Dostawca usługi cyfrowej | **Podmiot publiczny**

Czy reprezentowany przez Państwa podmiot publiczny jest jednocześnie operatorem usługi kluczowej?

Zgodnie z art 25 ustawy z dnia 5 lipca 2018 (Dz. U. poz. 1560) o krajowym systemie cyberbezpieczeństwa, podmioty, wobec których wydana została odpowiednia decyzja podlegają pod tryb zgłaszania przewidziany dla operatorów usług kluczowych.

Jeśli reprezentowany przez Państwa podmiot publiczny nie figuruje w wykazie operatorów usług kluczowych, prosimy o wybranie opcji "Podmiot publiczny".

Podmiot publiczny
Reprezentowany przeze mnie podmiot nie jest operatorem usługi kluczowej.

⚠ Podmiot publiczny będący operatorem usługi kluczowej
Reprezentowany przeze mnie podmiot publiczny jest równocześnie operatorem usługi kluczowej.

CERTYFIKACJA RODO

Przedmiot: Proces przetwarzania danych.

Wytyczne EROD 1/2018 w sprawie certyfikacji i określenia kryteriów certyfikacji zgodnie z art. 42 i 43 rozporządzenia

Wytyczne EROD 4/2018 w sprawie akredytacji podmiotów certyfikujących na podstawie art. 43 ogólnego rozporządzenia o ochronie danych (2016/679)

Możliwość zatwierdzenia przez Prezesa UODO kryteriów certyfikacji

Prezes UODO nie wydał dodatkowych wymogów akredytacji podmiotów certyfikujących

KONKLUZJE

Rozporządzenie 2019/881 (Akt o cyberbezpieczeństwie). Określa ramy ustanawiania europejskich programów certyfikacji cyberbezpieczeństwa w celu zapewnienia odpowiedniego poziomu cyberbezpieczeństwa produktów ICT, usług ICT i procesów ICT w Unii oraz w celu uniknięcia rozdrobnienia rynku wewnętrznego w zakresie programów certyfikacji cyberbezpieczeństwa w UE.

Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa (ECCG), która m.in. doradza i pomaga KE przy pracach nad zapewnieniem spójnego wprowadzania i stosowania ram certyfikacji cyberbezpieczeństwa, w szczególności w odniesieniu do unijnego kroczącego programu prac, kwestii związanych z polityką certyfikacji cyberbezpieczeństwa, koordynacji koncepcji politycznych oraz przygotowywania europejskich programów certyfikacji cyberbezpieczeństwa; zajmie się uregulowaniem europejskich ram certyfikacji cyberbezpieczeństwa na poziomie unijnym celem zwiększenia zaufania obywateli i przedsiębiorców do jednolitego rynku cyfrowego.

Grupa Interesariuszy ds. Certyfikacji Cyberbezpieczeństwa m.in. doradza KE w sprawie strategicznych kwestii związanych z europejskimi ramami certyfikacji cyberbezpieczeństwa.

W lutym 2018 Polska dołączyła do grupy państw sygnatariuszy porozumienia SOGIS (Senior Official Group Information Security Systems), Przygotowywany jest także pierwszy europejski program certyfikacji EUCC, również oparty o kryteria oceny zabezpieczeń informatycznych.

CZAS ZGŁOSZENIA NARUSZENIA RODO

72h

CZAS ZGŁOSZENIA INCYDENTU CyberBezpU

24h

KONKLUZJE

Dziękujemy za uwagę