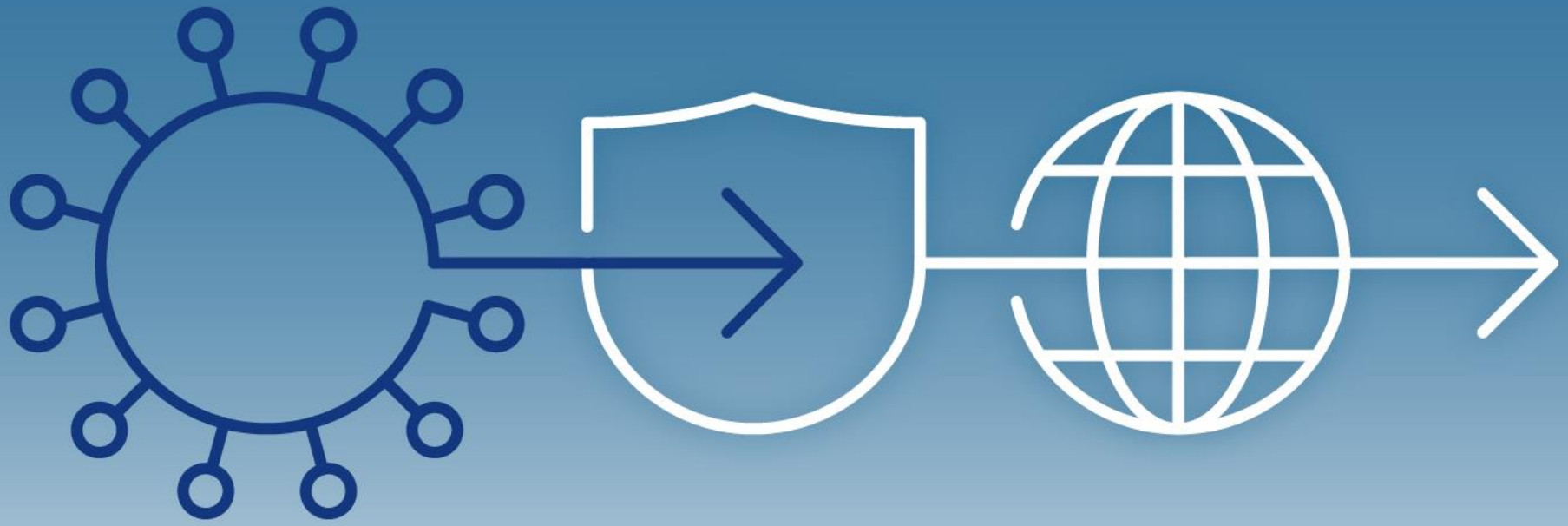
Konferencja Naukowa Bezpieczeństwo w Internecie – Cyberpandemia

22-23 października 2020 r.



Sektorowa Rada ds. Kompetencji
Telekomunikacja i Cyberbezpieczeństwo

UNIWERSYTET KARDYNAŁA STEFANA WYSZYŃSKIEGO W WARSZAWIE

POLSKIE TOWARZYSTWO INFORMATYCZNE

Naukowe Centrum Prawno-informatyczne

Cyberbezpieczeństwo a ochrona danych

Dr hab. Arwid Mednis

Wydział Prawa i Administracji

Uniwersytet Warszawski

Ochrona danych osobowych i cyberbezpieczeństwo – zakres obowiązywania przepisów

- **Przepisy o ochronie danych osobowych** obowiązują w zdecydowanej większości podmiotów
- Obowiązki wynikają głównie z RODO
- Przepisy o tajemnicach sektorowych, zawodowych

Cel: ochrona praw i wolności

- **Przepisy o cyberbezpieczeństwie** dotyczą określonych grup podmiotów:
  - Operatorzy usług kluczowych
  - Dostawcy usług cyfrowych
  - Podmioty publiczne
- Obowiązki wynikają z Ustawy o krajowym systemie cyberbezpieczeństwa (UKSC)

Cel: bezpieczeństwo i ciągłość świadczenia usług

Ochrona danych osobowych – najważniejsze grupy obowiązków

- Zasady ogólne (m. in. minimalizacja, okresy przechowywania danych)
- Obsługa praw podmiotów danych
- Ocena skutków przetwarzania
- Privacy by default
- Privacy by design
- Bezpieczeństwo danych osobowych
- Obsługa naruszeń
- Współpraca z organem nadzorczym

Cyberbezpieczeństwo – główne obowiązki

Operatorzy usług kluczowych:

- System zarządzania bezpieczeństwem informacji
- Szacowanie i zarządzanie ryzykiem
- Wdrożenie odpowiednich środków bezpieczeństwa
- Zarządzanie incydentami
- Współpraca z organem właściwym i CSIRT
- Dokumentacja systemu informacyjnego
- Struktury wewnętrzne odpowiedzialne za cyberbezpieczeństwo
- Audyty

Dostawcy usług cyfrowych:

- Zarządzanie ryzykiem
- Obsługa incydentu
- Zgłaszanie incydentów
- Bezpieczeństwo sieci i systemów informatycznych
- Zarządzanie ciągłością działania
- Monitorowanie, testowanie, audyty

Podmioty publiczne – główne obowiązki z zakresu cyberbezpieczeństwa

- Wyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa
- Zarządzanie, zgłaszanie i obsługa incydentów
- Współpraca i wymiana informacji z CSIRT

Inspektor ochrony danych

Obowiązek wyznaczenia IOD, gdy:

- Przetwarzania dokonują **organ lub podmiot publiczny**, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości
- Główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają **regularnego i systematycznego monitorowania** osób, których dane dotyczą, na dużą skalę; lub
- Główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu **na dużą skalę szczególnych kategorii danych osobowych oraz danych osobowych dotyczących wyroków skazujących i naruszeń** prawa

Rola IOD: monitorowanie przestrzegania przepisów o ochronie danych, informowanie administratora, współpraca z organem nadzorczym. Nie jest rekomendowane łączenie funkcji IOD z odpowiedzialnością za cyberbezpieczeństwo.

Ochrona danych osobowych a cyberbezpieczeństwo

Główne obszary wspólne:

- Zarządzanie ryzykiem (ocena skutków przetwarzania)
- Zarządzanie incydentami (naruszenia ochrony danych osobowych)

Obszary i środki organizacyjne:

- Polityki i procedury (np. procedura obsługi incydentów)
- Współpraca IOD i głównych osób odpowiedzialnych za ochronę danych z działem bezpieczeństwa

Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo

UNIWERSYTET KARDYNAŁA STEFANA WYSZYŃSKIEGO W WARSZAWIE

POLSKIE TOWARZYSTWO INFORMATYCZNE

Naukowe Centrum Prawno-informatyczne

Dziękuję za uwagę

a.mednis@wpia.uw.edu.pl