Zadanie
„Model normatywny podnoszenia kompetencji cyfrowych w szkołach wyższych”
finansowane w ramach dotacji celowej pochodzącej ze środków Ministerstwa Edukacji i Nauki na podstawie Umowy Nr MEiN/2023/CTC/2625

Konferencja naukowa
„Wzmacnianie odporności szkół wyższych
na cyberataki przez podnoszenie kompetencji cyfrowych”

Ochrona danych osobowych i informacji niejawnych w szkołach wyższych

Prelegent: Piotr Drobek, UKSW

Ministerstwo Edukacji i Nauki

UKSW Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie

CLTC Centrum Liderów Transformacji Cyfrowej

Podstawy prawne ochrony danych osobowych

- Konstytucja RP (art. 51)
- Ogólne rozporządzenie o ochronie danych (RODO)
- Ustawa z 10.05.2018 r. o ochronie danych osobowych
- Ustawa z 14.12.2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości
- Ustawa z 20.07.2018 r. o szkolnictwie wyższym i nauce (dział XIV a – Przetwarzanie danych osobowych – art. 469a i 469b)

Dane osobowe

Wszelkie informacje

O (dotyczące)

Zidentyfikowanej lub możliwej do zidentyfikowania

Osobie fizycznej

Nowe podejście do ochrony danych

- Dostosowanie zasad ochrony danych do aktualnego stanu wiedzy
- Podejście oparte na ryzyku (prawdopodobieństwo naruszenia praw lub wolności osoby, której dane dotyczą) – nie zastępuje zasad przetwarzania danych
- Rozliczalność – wdrożenie (operacjonalizacja zasad ochrony danych w działalności organizacji) i zdolność do wykazania przestrzegania przepisów o ochronie danych

Szkoła wyższa jako administrator danych

- **Administrator** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który **samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.**
- Jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

Szkoła wyższa jako administrator danych

- Współadministrowanie
- Powierzenie przetwarzania danych
- Platformy internetowe

Zasady przetwarzania danych

- Zgodność z prawem, rzetelność, przejrzystość
- Ograniczenie celu
- Minimalizacja danych
- Prawidłowość danych
- Ograniczenie przechowywania
- Integralność i poufność
- Rozliczalność

Zasady przetwarzania danych

- Zgodność z prawem, rzetelność, przejrzystość
- Ograniczenie celu
- Minimalizacja danych
- Prawidłowość danych
- Ograniczenie przechowywania
- Integralność i poufność
- Rozliczalność

Rozliczalność

Rozliczalność

czyli

Obowiązek przestrzegania zasad ochrony danych
i zdolność do wykazania tego

Poprzez wdrożenie wewnętrznych mechanizmów i procedur

Art. 5 ust. 2 należy czytać łącznie z art. 24 i 25

Rozliczalność

- ***Accountability*** **–** problem z tłumaczeniem na inne języki niż język angielski, w których różne wymiary odpowiedzialności określa się zazwyczaj jednym słowem. ***Accountability*** **tłumaczy się na j. polski jako *rozliczalność* lub *odpowiedzialność*.**
- Najlepiej sens tego pojęcia oddaje termin hiszpański: responsabilidad proactiva (**odpowiedzialność proaktywna**)
- Od teorii do praktyki – mechanizm zapewniający operacjonalizację zasad ochrony danych w praktyce działania organizacji.
- Mechanizm zarządzania ochroną danych osobowych w organizacji.
- Mechanizmy oparte na zasadzie rozliczalności nie zastępują zasad przetwarzania danych.
- Opinia GR 29 Opinia 3/2010 w sprawie zasady rozliczalności

Rozliczalność – art. 24 RODO

1.Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

2.Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

3.Stosowanie zatwierdzonych kodeksów postępowania, o których mowa wart. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa wart. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.

Inspektor Ochrony Danych

- Obowiązek wyznaczenia przez organ lub podmiot publiczny
- m.in. Monitoruje przestrzeganie RODO i podejmuje działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty
- Administrator oraz podmiot przetwarzający zapewniają, **by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych**
- Niezależność IOD

Bezpieczeństwo danych

Do 24 maja 2018 r. obowiązywało Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W konsekwencji wprowadzenia zasady rozliczalności nie ma szczegółowych regulacji prawnych w tym zakresie.

- Wyjaśnienia i opinie Prezesa UODO, EROD, ENISA
- Pomocniczo standardy ISO
- Podmioty publiczne - ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa

Kodeksy postępowania

Art. 40 ust. 1. Państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają do sporządzania kodeksów postępowania **mających pomóc we właściwym stosowaniu niniejszego rozporządzenia** – z uwzględnieniem specyfiki różnych sektorów dokonujących przetwarzania oraz szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.

Motyw 98 Należy zachęcać zrzeszenia lub inne organy reprezentujące kategorie administratorów lub podmiotów przetwarzających do sporządzania kodeksów postępowania, w granicach niniejszego rozporządzenia, by **ułatwiać skuteczne stosowanie niniejszego rozporządzenia**, z uwzględnieniem szczególnych cech przetwarzania prowadzonego w niektórych sektorach i szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.
W takich kodeksach można w szczególności **dopasować obowiązki administratorów i podmiotów przetwarzających do ryzyka naruszenia praw lub wolności osób fizycznych, jakie może powodować przetwarzanie**.

„wartość dodana” kodeksów postepowania

Kodeksy postępowania – zakres podmiotowy

- Zrzeszenia lub inne organy reprezentujące kategorie administratorów lub podmiotów przetwarzających
- Sektor: publiczny i prywatny (także kodeksy obejmujące podmioty z obu sektorów)

Kodeksy postępowania – rodzaje

- Krajowe
- Transgraniczne (Transnarodowe)
- Kodeksy, co do którego KE stwierdziła powszechne obowiązywanie w UE
- Wykorzystywane do międzynarodowych transferów danych

Prace nad kodeksami postępowania w szkolnictwie wyższym

- Kodeks postępowania w zakresie przetwarzania danych osobowych przez uczelnie publiczne – środowiskowy projekt regulacji
- Kodeks postępowania w zakresie ochrony danych osobowych (dla Uczelni Medycznych) - Konferencja Rektorów Akademickich Uczelni Medycznych
- Kodeks postępowania w sprawie przetwarzania danych osobowych dla celów badań naukowych przez biobanki w Polsce

Podstawy prawne ochrony informacji niejawnych

- Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych
- Rozporządzenie Prezesa Rady Ministrów z dnia 27 kwietnia 2011 r. w sprawie przygotowania i przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych
- Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego
- Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne
- Rozporządzenie Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych
- Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzuli tajności
- Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych

Informacje niejawne

Informacje, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażenia.

System ochrony informacji niejawnych

- Bezpieczeństwo fizyczne
- Bezpieczeństwo osobowe
- Bezpieczeństwo obiegu dokumentów i nośników informacji
- Bezpieczeństwo teleinformatyczne

Dziękuję za uwagę