# Outsourcing szansą i zagrożeniem w świetle RODO oraz wyzwanie dla ADO

Ryszard Piesak
ryszard.piesak@polsl.pl
Politechnika Śląska
Biuro Bezpieczeństwa Informacji

Adrian Kapczyński
adrian.kapczynski@polsl.pl
Politechnika Śląska
Wydział Matematyki Stosowanej

# Cele do zrealizowania

Politechnika Śląska

- RODO uświadomienie zagrożeń związanych z outsourcingiem, wyciekiem danych i odpowiedzialnością ADO

- Kiedy outsourcing może zmniejszyć  odpowiedzialność kierownictwa w świetle RODO?

# Rola informacji w dzisiejszym świecie

Politechnika Śląska

- Wartość informacji w organizacji
- Globalizacja i kradzież informacji
- Bezpieczeństwo przetwarzania (zapewnienie integralności, poufności, dostępności)
- Chaos informacyjny
- Konieczność weryfikacji źródeł, dezinformacja

# Definicja z RODO

- „przetwarzanie” oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie

Art. 1 ust. 2

# Definicja z RODO

- „naruszenie ochrony danych osobowych” oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych

Art. 4 ust.12

# Art. 32
*bezpieczeństwo przetwarzania*

2. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Sankcje za naruszenie zasad bezpieczeństwa przetwarzania;

- Do 20 milionów euro lub do 4% wartości rocznego światowego obrotu przedsiębiorstwa

# Kradzież wzrokowa zdemaskowana

Wyniki globalnego eksperymentu kradzieży wzrokowe

Przeprowadzono tajny eksperyment, w którym haker wzrokowy został wysłany do biur w ośmiu różnych krajach. Celem było wykazanie, jak łatwo jest wykraść wzrokowo wrażliwe dane firmy.

**Cel:** wykraść wrażliwe lub tajne informacje wykorzystując jedynie wzrok

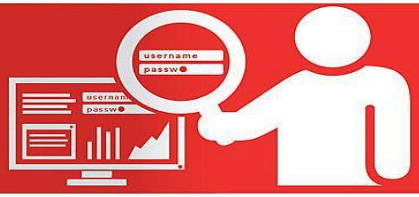
**Państwa uczestniczące:** Chiny, Francja, Niemcy, Indie, Japonia, Korea, Wielka Brytania, USA

Blisko połowa prób kradzieży wzrokowej zakończyła się sukcesem w czasie krótszym niż **15 min.**

**91%** prób kradzieży zakończyło się **sukcesem**

**Monitory komputerów pracowników** są narażone na kradzież wzrokową

**52%** wrażliwych informacji było przejętych z monitorów.




W przeliczeniu na każdą próbę zostało wzrokowo skradzionych średnio **3.9 informacji.**

**27%** informacji do których uzyskano dostęp, zawierało dane logowania, informacje finansowe oraz ważne i tajne dokumenty.

W **68%** sytuacji kradzież wzrokowa była niezauważona lub została zignorowana przez pracowników, co oznacza, że ochrona twojej firmy zależy od ciebie.

Ochrona wrażliwych danych za pomocą filtrów prywatyzujących 3M™

Dowiedź się więcej na www.chron-dane.pl

Przy tłumaczeniu wykorzystano: http://solutions.3mpoland.pl/wps/portal/3M/pl_PL/Protectors/Home/Sektroy/Haker-Wzrokowy-Zdemaskowany/

**The experts in screen privacy.** | 3M

Politechnika Śląska

# Incydenty bezpieczeństwa.
## *Kto za tym stoi?*

Politechnika Śląska

- Nieznany sprawca
- Pracownicy
- Podwykonawcy
- Tylko kilka procent przedsiębiorców jest zadowolonych z kompetencji swoich służb IT w aspekcie bezpieczeństwa
- Większość  nie otrzymuje pełnej informacji  o incydentach bezpieczeństwa

*Źródło: opracowanie własne*

# Ile warte są dane ?

## *Europa traci 65 mld euro na cyberprzestępczości*

Politechnika Śląska

- *Dane obywateli Unii Europejskiej są więcej warte. Hakerzy wyceniają je od 25 do 40 dolarów. Są to jedne z najdroższych informacji jakie można kupić w darknecie, obok europejczyków równie dużo płaci się za obywateli Kanady (od 20 do 40$) i Australii (od 21$ do 40$).*
- *Obejmuje on numer konta, datę urodzenia właściciela katy, numer PIN, adres domowy, a nawet nazwisko panieńskie matki właściciela. Oczywiście za taką pełną informację hakerzy żądają więcej. Za podstawowe dane Amerykanina płaci się około 8 dolarów. Kiedy zażyczymy sobie opcję "full wypas" zawierającą dokładne dane użytkownika wtedy taka paczka kosztuje nas nawet 45 dolarów.*
- *Eksperci uważają, że nie ma co liczyć na skuteczne śledztwo policji.*
- *Zasoby, jakimi dysponuje policja i prokuratura, są bowiem zbyt małe w porównaniu do możliwości przestępców.*

*Źródło: https://news.money.pl/artykul/europa;traci;65;mld;euro;na;cyberprzestepczosci,69,0,358213.html*

# Śmiertelnie groźny outsourcing

Politechnika Śląska

- Źle przeprowadzony outsourcing może okazać się bardzo groźny.
  - *Szwedzka Agencja Transportu, od kilku lat zmagała się z trudnościami finansowymi, związanymi z niedofinansowaniem oraz z koniecznością cięcia kosztów.*
  - *Nowa dyrektor generalna firmy postanowiła rozwiązać problem ostatecznie: dane firmy miały zostać przeniesione do chmury.*
  - *Zwolniono 3/4 działu IT oraz cały dział bezpieczeństwa.*
  - *Ta właśnie operacja stała się początkiem upadku zarówno dyrektor generalnej, jak i potężnego kryzysu politycznego.*
  - *Nikt nie był w stanie wytłumaczyć dyrektor generalnej, jakich danych wrażliwych nie wolno przekazywać na zewnątrz, wydane natomiast zostało polecenie, aby przekazać wszystkie dane, jakimi Agencja dysponuje.*
  - *Jako, że Agencja Transportu jest agendą państwową urządzono przetarg, który i tak wygrała firma dotychczas obsługująca Agencję, czyli IBM.*

*Źródło: http://biznes.interia.pl/raport/bezpiecznie-w-sieci/news/smiertelnie-grozny-outsourcing*

# Korzyści outsourcingu

Politechnika Śląska

- Oszczędności finansowe
- Odciążenie własnych zasobów
- Wykorzystanie ekspertów z zewnątrz możliwością rozwoju organizacji i zwiększenia bezpieczeństwa
- Możliwość transferu ryzyk i odpowiedzialności na dostawców

# Outsourcing okiem dostawcy

- Wykonać zlecenie maksymalnie korzystnie
- Problemy z własnymi zasobami „zdobywanie doświadczeń na zleceniodawcach”
- Szukanie najtańszych własnych poddostawców
- Walka z konkurencją z branży
- Zabezpieczenie własnych interesów na poziomie umowy (odpowiedniej klasy wsparcie prawne)
- Minimalizacja ryzyk i odpowiedzialności za wykonaną usługę

# Outsourcing w RODO: zagrożenia

Politechnika Śląska

- Ryzyko utraty know-how
- Niesolidny usługodawca, proponowanie rozwiązań przez tzw. ekspertów RODO”
- Nieodpowiednie kompetencje i potencjał oferenta
- Zwiększenie ryzyka wycieku, utraty lub kradzieży danych
- Uzyskanie najtańszego korzystającego z szablonowych rozwiązań dostawcy
- Nierealność egzekwowania odpowiedzialności w przypadku incydentu

# Outsourcing w RODO: zagrożenia

Politechnika Śląska

- Niezadowolony i uświadomiony pracownik
- Niezadowolony klient
- Nowe zagrożenie - kancelarie odszkodowawcze
- Możliwość uzależnienia od jednego dostawcy, brak alternatyw
- Brak lub niewłaściwe wewnętrzne procedury zabezpieczające
- Bezwład organizacyjny

# Outsourcing: usuwanie zagrożeń

Politechnika Śląska

- Odpowiednio zdefiniowana i zabezpieczająca interesy zamawiającego umowa z realną możliwością zastosowania „regresu”
- Przeprowadzenie analizy i akceptacja ryzyk w przypadku niewywiązania się z oferty
- Nadzór, szkolenia i kontrole usługodawców
- Prewencyjne korzystanie z doradztwa i wiedzy niezależnych ekspertów
- Korzystanie z merytorycznych zespołów kompetencyjnych
- Realna dbałość o ochronę informacji w organizacji

# Art. 28 ust.1
*Podmiot przetwarzający*

Politechnika Śląska

- 1. Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą.
- f). Uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art.32-36.
- g). Po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie …
- h). Udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzenie audytów, w tym inspekcji i przyczynia się do nich.

# CO wymusza RODO po 25.05.2018r.

Politechnika Śląska

- Wprowadzenie zmian organizacyjnych , technologicznych i prawnych
- Zwiększenie odpowiedzialności ADO i podmiotów przetwarzających
- Konieczność uwzględnienia ochrony danych osobowych już w fazie projektowania rozwiązań i inwestycji (art.25)
- Działania prewencyjne, zabezpieczenie własnych interesów dotyczących ochrony danych już na poziomie SIWZ (art.28)
- Skuteczny nadzór nad outsourcingiem – kontrole dostawców (art.28)
- Ciągłe szkolenia i tworzenie kultury bezpieczeństwa w organizacji

# Symulacja niektórych kosztów własnych związanych z RODO

**(od kilku do kilkuset tys. za każdy rekord**
**w zależności od wielkości organizacji i jakości usługi )**

Politechnika Śląska

- Audyt bezpieczeństwa danych
- Audyt wymogów RODO (przeprowadzenie audytu w zakresie spełnienia wymagań rozporządzenia o ochronie danych osobowych)
- Przeprowadzenie inwentaryzacji danych osobowych
- Poprawa i dostosowanie dotychczasowych umów do nowych wymagań
- Opracowanie nowych procedur i dokumentacji
- Szkolenia pracowników w zakresie nowych zasad ochrony danych osobowych (warto zwrócić uwagę na jakość)
- Dostosowanie systemów informatycznych do nowych wymagań prawnych
- Nadzór nad wdrożeniem RODO

*Źródło: opracowanie własne*

# Procesowe spojrzenie na wdrożenie RODO

Politechnika Śląska

- Potrzebne są:
  - budżet
  - czas
  - aktywne zaangażowanie całej organizacji
  - merytoryczne zespoły kompetencyjne
  - systemowe rozwiązania

# Oczekiwania wobec  Inspektora Ochrony Danych

Politechnika Śląska

- ADO oczekuje że IOD będzie miał kompetencje;
  - prawnika
  - informatyka
  - audytora
  - kontrolera
  - dydaktyka
  - doradcy, wykonawcy i organizatora procesów związanych ochroną danych osobowych

**Na ile je wycenia?**

# Art. 82.

3. Administrator lub podmiot przetwarzający zostaną zwolnieni z odpowiedzialności wynikającej z ust.2 jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody.

*“Zdolne do przetrwania są ani nie najsilniejsze,*
*ani nie najbardziej inteligentne gatunki*
*– to te, które najszybciej przystosowują się do zmian”*
*Karol Darwin*

Politechnika Śląska

**Dziękuję!**


Ryszard Piesak
tel. 662 366 388

Ryszard.Piesak@polsl.pl

Politechnika Śląska

Biuro Bezpieczeństwa Informacji