Urząd Ochrony Danych Osobowych

MONITORING WIZYJNY W SZKOLE

ASPEKTY PRAWNE I TECHNICZNE

IX edycja Ogólnopolskiego Programu Edukacyjnego

„Twoje dane – Twoja sprawa”

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.uodo.gov.pl
kancelaria@uodo.gov.pl

Urząd Ochrony Danych Osobowych

ASPEKTY PRAWNE

Krzysztof M. Król

Zespół Analiz i Strategii

Urząd Ochrony Danych Osobowych

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.uodo.gov.pl
kancelaria@uodo.gov.pl

PODSTAWY PRAWNE MONITOROWANIA

- **Art. 6 ust. 1 lit. e RODO** – wykonanie zadania realizowanego w interesie publicznym przez administratora

- **Art. 108a** ustawy z dnia 14 grudnia 2016 r. - **Prawo oświatowe** (Dz. U. z 2018 r. poz. 996 z późn. zm.) w zw. z art. 68 ust. 1 pkt 6 - doprecyzowanie zasad realizacji zadania dyrektora szkoły (placówki) – zapewnianie bezpiecznych warunków zajęć i pracy

- Przepisy doprecyzowują zasady nadzoru i dotyczą nowych oraz już istniejących systemów – tutaj konieczne jest dostosowanie.

SPOSÓB WPROWADZENIA MONITORINGU

- **w uzgodnieniu** z organem prowadzącym szkołę (placówkę)
- po przeprowadzeniu **konsultacji** z:
  - radą pedagogiczną,
  - radą rodziców,
  - samorządem uczniowskim.
  - +rada szkoły

- uzgodnienie z organem prowadzącym odpowiednich środków technicznych i organizacyjnych w celu ochrony przechowywanych nagrań

CELE PRZETWARZANIA DANYCH

- zapewnienie bezpieczeństwa uczniów i pracowników,
- ochrona mienia.
- Monitoring nie może być środkiem nadzoru nad jakością wykonywania pracy przez pracowników szkoły lub placówki.

SPOSÓB I OBSZAR NADZORU

- środki techniczne umożliwiające rejestrację obrazu
  - wyłączenie możliwości nagrywania dźwięku

- pomieszczenia szkoły (placówki) lub
- teren wokół szkoły (placówki)
  - zgodnie z zasadami ograniczenia celu i minimalizacji danych

Urząd Ochrony Danych Osobowych

OBSZARY WYŁĄCZONE Z NADZORU

- Pomieszczenia:
  - w których odbywają się zajęcia: dydaktyczne, wychowawcze i opiekuńcze;
  - w których uczniom udzielana jest pomoc psychologiczno-pedagogiczna,
  - przeznaczone do odpoczynku i rekreacji pracowników,
  - sanitarnohigieniczne;
- Gabinet profilaktyki zdrowotnej,
- Szatnie i przebieralnie,

- chyba że…

Urząd Ochrony Danych Osobowych

WYJĄTKOWE DOPUSZCZENIE NADZORU OBSZARÓW WYŁĄCZONYCH

- stosowanie monitoringu jest niezbędne ze względu na istniejące zagrożenie dla realizacji celów,
- nie naruszy to godności oraz innych dóbr osobistych uczniów, pracowników i innych osób,
- w szczególności poprzez zastosowanie technik uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób **– otwarty katalog rozwiązań**

OKRES PRZECHOWYWANIA NAGRAŃ

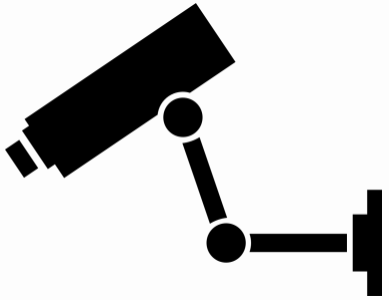
- okres nieprzekraczający 3 miesięcy od dnia nagrania,
- po upływie okresów nagrania zawierające dane osobowe podlegają zniszczeniu, o ile przepisy odrębne nie stanowią inaczej,
- za dopuszczalne należy uznać przechowywanie do prawomocnego zakończenia postępowań, w których nagrania incydentów stanowią dowód.

INFORMOWANIE OSÓB OBSERWOWANYCH

- poinformowanie uczniów i pracowników o monitoringu, w sposób przyjęty w szkole (placówce), nie później niż 14 dni przed jego uruchomieniem,
- poinformowanie na piśmie pracowników przed dopuszczeniem do pracy o stosowaniu monitoringu,
- oznaczenie pomieszczeń i terenu monitorowanego w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych - nie później niż jeden dzień przed jego uruchomieniem,
- **obowiązek zastosowania przepisów art. 12 i art. 13 RODO.**

PRZYKŁAD KLAUZULI INFORMACYJNEJ

Obiekt monitorowany/Teren monitorowany



Monitoring prowadzony jest przez szkołę podstawową nr 11, w celu zapewnienia bezpieczeństwa uczniów i pracowników oraz ochrony mienia i obejmuje korytarze oraz teren wokół budynku. Nagrania są przechowywane przez 7 dni. Więcej informacji można uzyskać: … *(pod numerem telefonu, w sekretariacie szkoły, od inspektora ochrony danych, strona www).*

Urząd Ochrony Danych Osobowych

PRAWA OSÓB OBSERWOWANYCH – ART. 15-21 RODO

- Prawo dostępu do nagrań
- Prawo do sprostowania danych – ograniczony zakres
- Prawo do usunięcia danych
- Prawo do ograniczenia przetwarzania
- Prawo do przenoszenia danych – nie ma zastosowania
- Prawo do sprzeciwu wobec przetwarzania

Urząd Ochrony Danych Osobowych

DOSTĘP DO NAGRAŃ

- osoby upoważnione przez administratora,
- osoby obserwowane w związku z realizacją ich praw i ich przedstawiciele,
- organy publiczne w ramach konkretnego postępowania prowadzonego na podstawie przepisów prawa,
- odbiorcy w związku z prawnie uzasadnionym interesem.

Urząd Ochrony Danych Osobowych

ŚRODKI TECHNICZNE I ORGANIZACYJNE

Monika Adamczyk

Zespół Analiz i Strategii

Urząd Ochrony Danych Osobowych

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.uodo.gov.pl
kancelaria@uodo.gov.pl

PLANOWANIE MONITORINGU WIZYJNEGO

Urząd
Ochrony
Danych
Osobowych

MONITORING WIZYJNY (TAK/NIE?)

PRZED WDROŻENIEM MONITORINGU WIZYJNEGO, DYREKTOR SZKOŁY LUB PLACÓWKI POWINIEN UZGODNIĆ Z ORGANEM PROWADZĄCYM SZKOŁĘ LUB PLACÓWKĘ ODPOWIEDNIE ŚRODKI TECHNICZNE I ORGANIZACYJNE W CELU OCHRONY PRZETWARZANYCH W NIM DANYCH

- czy **cel** monitoringu jest jasny, konkretny i jednoznaczny oraz czy ma podstawę prawną?
- jakie są **zalety** korzystania z monitoringu wizyjnego i czy przewyższają one **negatywne skutki**?
- **czy monitoring wizyjny jest absolutnie niezbędny oraz czy są dostępne mniej inwazyjne alternatywy do zrealizowania tego celu?**

Urząd Ochrony Danych Osobowych

OCHRONA DANYCH W FAZIE PROJEKTOWANIA

ODPOWIEDNIE ŚRODKI TECHNICZNE I ORGANIZACYJNE MUSZĄ BYĆ UWZGLĘDNIONE JUŻ NA ETAPIE PLANOWANIA MONITORINGU WIZYJNEGO

- **projekt i specyfikacja systemu** powinny przygotowane i zawierać między innymi **wymogi dla przetwarzania danych osobowych** zgodnie z przepisami prawa
- jeśli planowany jest **zakup komercyjnego systemu**, wymagania te muszą być zawarte w **specyfikacji zakupu**

DOMYŚLNA OCHRONA DANYCH

- **przetwarzanie wyłącznie tych danych osobowych, które są niezbędne** dla osiągnięcia każdego konkretnego celu przetwarzania
- zgodność z wymaganiami ochrony danych musi być zastosowana wobec **wszystkich komponentów systemu i przetwarzanych danych**, podczas **całego cyklu ich życia**
- gwarancje te powinny być wbudowane nie tylko w specyfikacje systemowe, ale również w **polityki i procesy organizacyjne**
- zapewnienie adekwatnego **poziomu świadomości** wśród personelu oraz osób monitorowanych na temat **celów i zasad monitoringu wizyjnego**

OCENA SKUTKÓW – KIEDY WYMAGANA?

OCENA SKUTKÓW JEST OBOWIĄZKOWA JEŻELI PRZETWARZANIE DANYCH MOŻE SPOWODOWAĆ WYSOKIE RYZYKO DLA PRAW I WOLNOŚCI OSÓB FIZYCZNYCH, W SZCZEGÓLNOŚCI DLA:

- systematycznego monitorowania na dużą skale miejsc dostępnych publicznie **wykorzystujące elementy rozpoznawania cech lub właściwości obiektów, które znajda się w monitorowanej przestrzeni** (np. systemy pozwalające na automatyczną identyfikację pojazdów wjeżdżających na parking)
- przetwarzania **szczególnych kategorii danych osobowych** (np. systemy kontroli wejścia oparte na biometrii wizualnej)

Urząd Ochrony Danych Osobowych

OCENA SKUTKÓW – JAK TO ZROBIĆ?

W RAMACH OCENY SKUTKÓW NALEŻY:

- **Opisać planowane operacje** przetwarzania i cele przetwarzania oraz gdy ma zastosowanie prawnie uzasadnione interesy realizowane przez administratora
- Dokonać oceny, czy **przetwarzanie jest niezbędne** oraz **proporcjonalne** w stosunku do określonych celów
- Przeprowadzić **analizę ryzyka** naruszenia praw lub wolności osób, których dane dotyczą
- **Zaplanować działania w celu zaradzenia ryzyku**, w tym **środki i mechanizmy bezpieczeństwa** mające zapewnić ochronę danych osobowych i wykazać przestrzeganie przepisów RODO

OCENA SKUTKÓW – CO POTEM?

NA PODSTAWIE UZYSKANYCH WYNIKÓW NALEŻY:

- Dokonać modyfikacji polityk, procedur i procesów dla monitoringu wizyjnego
- Zastosować niezbędne środki bezpieczeństwa dla ochrony danych i dla zminimalizowania zidentyfikowanych ryzyk

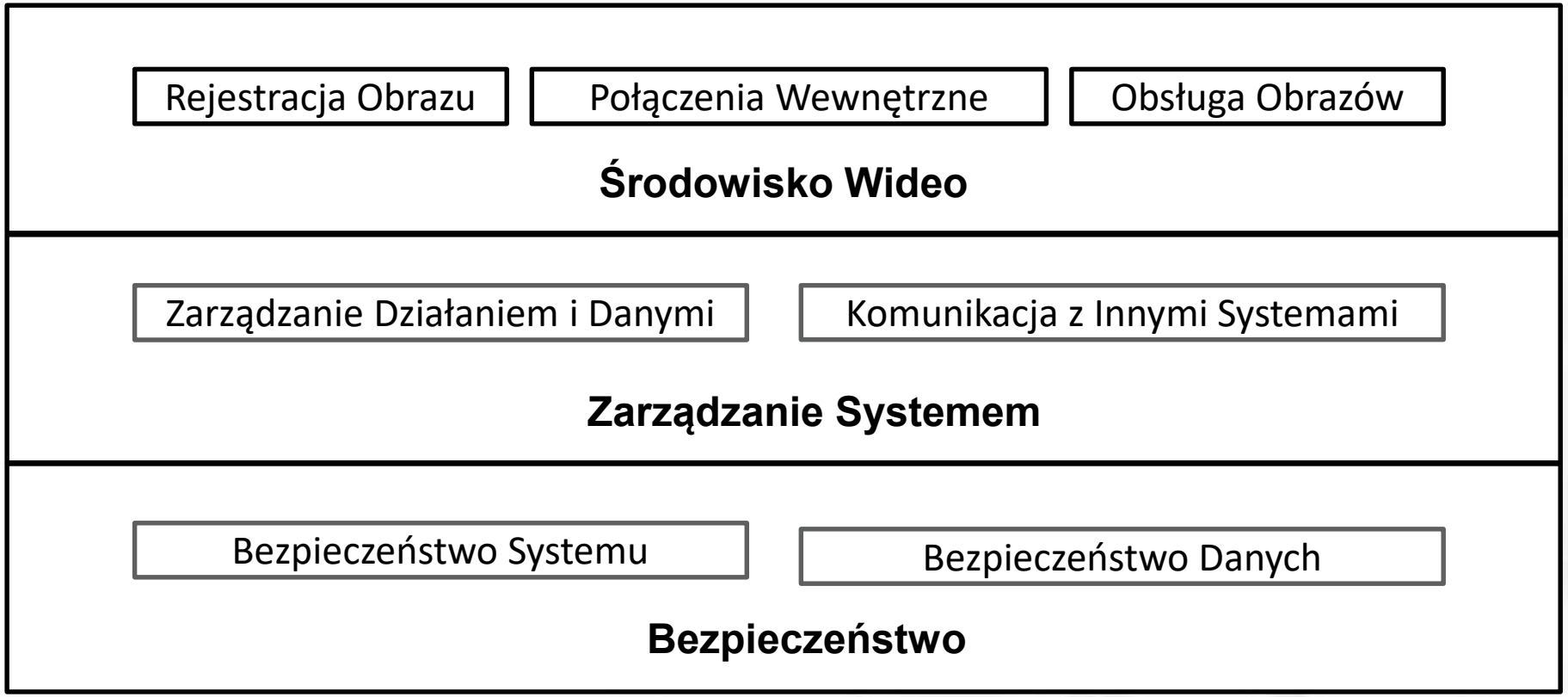
UPRZEDNIE KONSULTACJE

- Jeżeli wyniki oceny skutków dla ochrony danych wykażą, że **przetwarzanie spowodowałoby wysokie ryzyko pomimo zastosowanych środków bezpieczeństwa**, konieczne będzie **skonsultowanie się z UODO przed rozpoczęciem przetwarzania**

BEZPIECZEŃSTWO MONITORINGU WIZYJNEGO

Urząd
Ochrony
Danych
Osobowych

SYSTEM MONITORINGU WIZYJNEGO



Urząd Ochrony Danych Osobowych

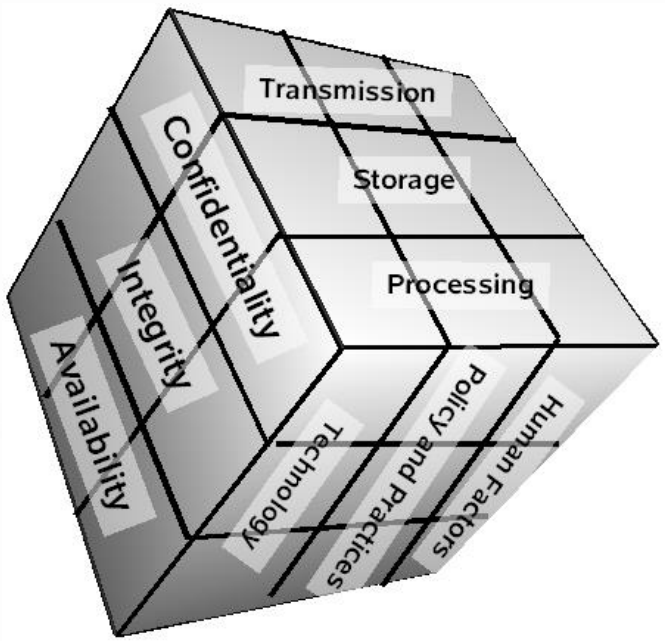
MODEL BEZPIECZEŃSTWA

KRYTYCZNE ATRYBUTY INFORMACJI

- Poufność (confidentiality)
- Integralność (integrity)
- Dostępność (availability)

STANY INFORMACJI

- Przesyłanie (transmission)
- Przechowywanie (storage)
- Przetwarzanie (processing)



ŚRODKI BEZPIECZEŃSTWA

- Organizacyjne (policy and practices)
- Technologiczne (technology)
- Ludzkie (human factors)

KRYTYCZNE ATRYBUTY INFORMACJI

POUFNOŚĆ to zapewnienie, że dane nie są celowo lub przypadkowo udostępniane nieupoważnionym podmiotom

INTEGRALNOŚĆ to zapewnienie, że dane nie zostały przypadkowo lub celowo zmodyfikowane w taki sposób, aby podważyć ich wiarygodność

DOSTĘPNOŚĆ to zapewnienie, że upoważnione osoby mają w razie potrzeby szybki i niezawodny dostęp do potrzebnych danych

STANY INFORMACJI

PRZESYŁANIE to przekazywanie danych między systemami informatycznymi (zwane również danymi w tranzycie)

PRZECHOWYWANIE to dane w stanie spoczynkowym w systemie informacyjnym, np. przechowywane w pamięci komputera, na twardym dysku lub mobilnym nośniku (CD, pendrive)

PRZETWARZANIE to wykonywanie operacji na danych aby móc osiągnąć pożądany cel przetwarzania

ŚRODKI BEZPIECZEŃSTWA

ORGANIZACYJNE to polityki i procedury definiujące i regulujące cele i sposoby używania informacji (np. dopuszczalne zasady ich wykorzystywania lub procedury reagowania na incydenty naruszenia)

TECHNOLOGICZNE to rozwiązania sprzętowe i oprogramowanie wykorzystywane w celu ochrony informacji i systemów informatycznych

LUDZKIE to zapewnienie, przy pomocy szkoleń i treningów, że użytkownicy systemów przetwarzania danych są świadomi swoich ról i obowiązków oraz wiedzą jak przestrzegać przyjęte zasady

BEZPIECZEŃSTWO SYSTEMU MONITORINGU WIZYJNEGO

- Wykrywanie awarii i uszkodzeń komponentów, oprogramowania, połączeń wewnętrznych i międzysystemowych
- Ochrona przed manipulacją, modyfikacją i sabotażem systemu
- Ochrona przed nieautoryzowanym dostępem do systemu
- Ochrona przed nieautoryzowanym dostępem do danych we wszystkich ich stanach: przechowywanie, transmisja i przetwarzanie
- Zapewnienie poprawnej identyfikacji danych (np. ich źródła, daty i godziny utworzenia lub ich ostatniej modyfikacji)
- Ochrona przed modyfikacją lub usunięciem istniejących danych oraz przed wprowadzeniem fałszywych danych

POLITYKA I PROCEDURY BEZPIECZEŃSTWA 1/2

- Cel i zakres monitoringu wizyjnego
- Kto jest odpowiedzialny za zarządzanie monitoringiem wizyjnym
- Zasady i procedury kontroli dostępu do monitoringu wizyjnego (udzielanie, zmiana i odbieranie uprawnień)
- Dozwolone i niedozwolone stosowanie monitoringu wizyjnego (np. miejsca / czas kiedy jest on dozwolony a kiedy nie, korzystanie z ukrytych kamer oraz nagrywanie audio)
- Zasady rejestrowania wideo i czas jego przechowywania, w tym archiwizowanie nagrań wideo związanych z incydentami bezpieczeństwa

POLITYKA I PROCEDURY BEZPIECZEŃSTWA 2/2

- Procedury dla operatorów (np. rozpoczynanie i zakańczanie pracy, przez kogo i skąd nadzorowany jest system monitoringu)
- Zasady kto i kiedy musi przejść odpowiednie szkolenia
- Oznakowanie używane do informowania ludzi o prowadzonym monitoring wizyjnym
- Procedury zarządzania incydentami i przywracania dostępności do systemu i danych na wypadek awarii
- Procedury w przypadku żądań dostępu do nagrań wideo przez osoby trzecie
- Procedury dotyczące zamówień, instalacji i konserwacji systemu monitoringu wizyjnego

TECHNICZNE ZABEZPIECZENIA 1/2

- Zabezpieczenie całej infrastruktury (w tym też zdalnych kamer, okablowania i zasilania) przed fizycznymi manipulacjami, uszkodzeniami i ich kradzieżą
- System logicznej kontroli dostępu monitorujący logowanie się do niego, w szczególności wielokrotne nieudane próby
- Bezpieczne kanały komunikacyjne (fizyczne i logiczne) w celu ochrony materiału wideo przed przechwyceniem podczas jego transmisji
- Szyfrowanie przechowywanych nagrań wideo

TECHNICZNE ZABEZPIECZENIA 2/2

- Zapory ogniowe i oprogramowania antywirusowe
- Systemy wykrywania cyber ataków
- Systemy wykrywania awarii komponentów, oprogramowania i łącz komunikacyjnych
- Systemy redundancji i kopii zapasowych dla przywrócenia dostępności do systemu i danych na wypadek awarii

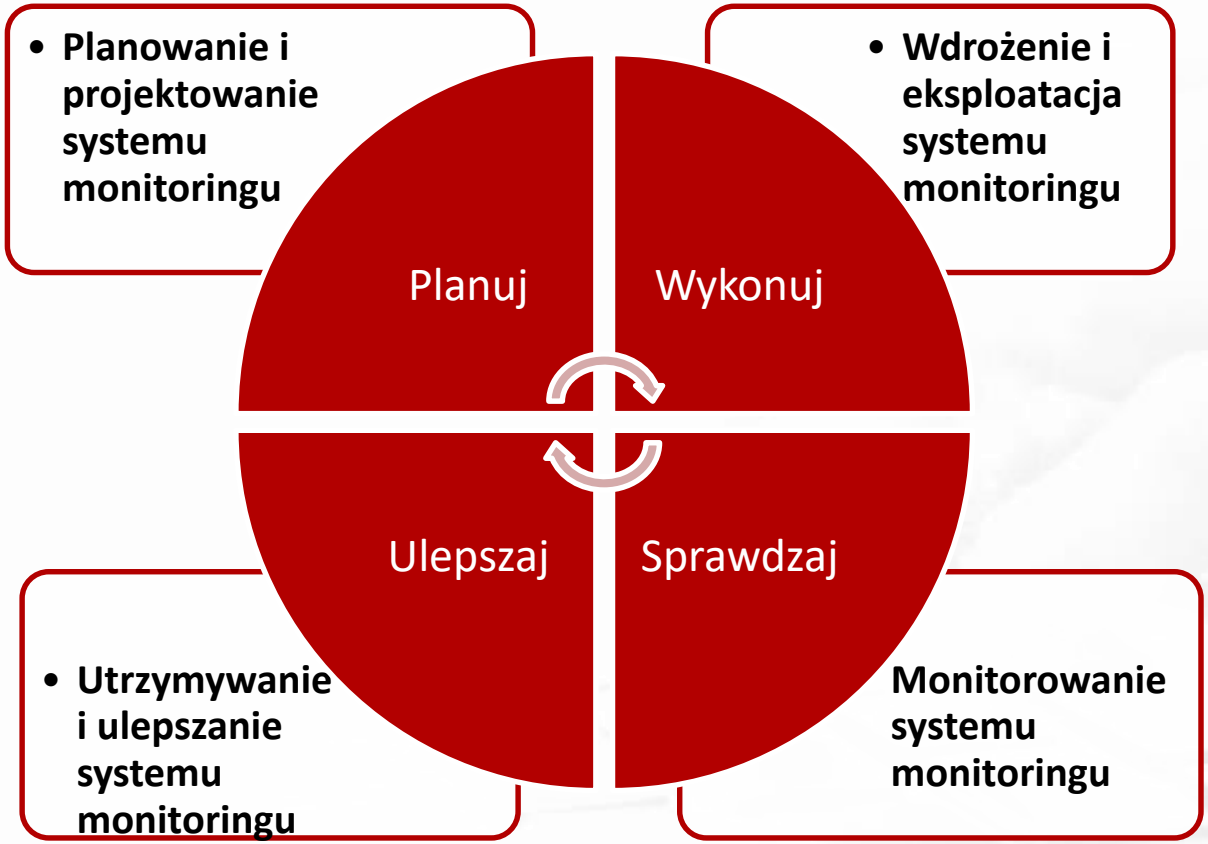
NAJSŁABSZYM OGNIWEM SYSTEMU BEZPIECZEŃSTWA ZWYKLE JEST CZŁOWIEK

- Brak zrozumienia dlaczego monitoring wizyjny jest stosowany
- Brak wiedzy i kompetencji w zakresie bezpieczeństwa informacji
- Błędy ludzkie spowodowane np. nieuwagą lub zmęczeniem
- Świadome działania pracowników (tzw. insider thread)
- Ataki przy pomocy metod socjotechniki i inżynierii społecznej w celu zdobycia informacji

ALE CZŁOWIEK MOŻE BYĆ JEDNYM Z NAJLEPSZYCH ŚRODKÓW BEZPIECZEŃSTWA

- Regularna edukacja na temat odpowiedzialnego i bezpiecznego przetwarzania danych
- Ciągłe budowanie świadomości, że zagrożenie jest realne – w jaki sposób je identyfikować i jak na nie reagować
- Kultura otwartości – zachęcanie pracowników do zgłaszania zauważonych naruszeń bez negatywnych konsekwencji
- Poprawne relacje – zespół ds. bezpieczeństwa i dział IT powinny być postrzegane jako zaufani i pomocni doradcy, a nie kontrolerzy i wrogowie

OCHRONA DANYCH W MONITORINGU WIZYJNYM TO CIĄGŁY PROCES



Urząd Ochrony Danych Osobowych

PODSUMOWANIE

- Wdrożenie monitoringu wizyjnego wymaga **starannego rozważenia i zaplanowania** przed podjęciem konkretnych działań
- System monitoringu wizyjnego to nie tylko kamery, ale też kable, systemy zapisu i odtwarzania nagrań
- Ochrona danych wymaga kompleksowego podejścia (**ludzie, technologie i środki organizacyjne**)
- System zabezpieczeń nie jest mocniejszy niż jego najsłabszy element
- **Ochrona danych to ciągły proces a nie produkt**

PRZYDATNE DOKUMENTY ORGANÓW

- Monitoring wizyjny w szkole – materiały edukacyjne VII edycji Programu „Twoje dane – Twoja sprawa”
  https://giodo.gov.pl/1520061/id_art/9851/j/pl

- Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystania monitoringu wizyjnego
  https://uodo.gov.pl/pl/138/354

- Wykorzystanie monitoringu wizyjnego w szkołach i jego wpływ na bezpieczeństwo uczniów (nr P/16/076) - informacje o wynikach kontroli Naczelnej Izby Kontroli
  https://www.nik.gov.pl/kontrole/P/16/076/LLU/https://uodo.gov.pl/pl/138/354

Urząd
Ochrony
Danych
Osobowych

PYTANIA?

DZIĘKUJEMY ZA UWAGĘ

TDTS@UODO.GOV.PL

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.uodo.gov.pl
kancelaria@uodo.gov.pl