

# MONITORING WIZYJNY A ODPOWIEDZIALNOŚĆ DYREKTORA. JAK PRZYGOTOWAĆ PLACÓWKĘ EDUKACYJNĄ DO KONTROLI MONITORINGU



## MOTYW 39 PREAMBUŁY

- Należy ograniczyć się do przetwarzania danych niezbędnych, bez których nie da się osiągnąć zamierzonego celu przetwarzania. (motyw 39 preambuły), zgodnie z którym dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami



# PRZETWARZANIE

- „**przetwarzanie**” oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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;



# Artykuł 6 – Zgodność przetwarzania z prawem

- 1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:
  - a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
  - b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
  - c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;





# Artykuł 6 – Zgodność przetwarzania z prawem

- 1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:
- d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
- e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.
- Akapit pierwszy lit. f) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.



# Jak RODO definiuje administratora danych(ADO)

- Artykuł 4 rozporządzenia stanowi:
- „(...) administratorem jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Natomiast 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”.



# „podmiot przetwarzający”

- Artykuł 4 rozporządzenia stanowi:

oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;



# Zapewnienie bezpieczeństwa danych

- RODO stawia przed administratorami danych szereg wyzwań: obowiązek uwzględniania i rozliczania przestrzegania zasad ochrony danych osobowych,
- obowiązek realizacji żądań osób, których dane dotyczą,
- obowiązek dokonywania oceny skutków planowanych operacji przetwarzania danych,
- obowiązek rejestrowania czynności przetwarzania danych,
- obowiązek współpracy z organem nadzorczym,
- obowiązek zgłaszania naruszenia ochrony danych osobowych, konsultowanie rozpoczęcia przetwarzania danych osobowych z organem nadzorczym oraz wyznaczenie inspektora ochrony danych jako czynność obligatoryjna w niektórych przypadkach a nie wyłącznie fakultatywna.





KPA Ustawodawca zdecydował, że obowiązek informacyjny (art. 13 RODO) musi być spełniony przez Organ administracji publicznej:

- **Obowiązek informacyjny – odpowiedź w KPA**



# KPA Ustawodawca zdecydował, że obowiązek informacyjny (art. 13 RODO) musi być spełniony przez Organ administracji publicznej:

- przy pierwszej czynności skierowanej do strony: przy wezwaniu (art. 54 § 1a kpa), (art. 61 § 5 kpa), przy zawiadomienie o przekazaniu sprawy (art. 65 § 1a kpa), przy zawiadomieniu wnoszącego podanie, że w sprawach innych powinien wnieść odrębne podanie do właściwego organu (art. 66 § 1 zdanie trzecie kpa), przy wydawaniu zaświadczenia na żądanie osoby ubiegającej się o zaświadczenie (art. 217a kpa) - chyba, że strona posiada te informacje, a ich zakres lub treść nie uległy zmianie,



# KPA Ustawodawca zdecydował, że obowiązek informacyjny (art. 13 RODO) musi być spełniony przez Organ administracji publicznej:

- przy wydaniu postanowienie o odmowie wszczęcia postępowania (art. 61a w § 1 zdanie drugie kpa),
- poprzez udostępnienie wymaganych informacji w Biuletynie Informacji Publicznej na swojej stronie podmiotowej, na swojej stronie internetowej oraz w widocznym miejscu w swojej siedzibie, w sprawach załatwianych milcząco.
- Przy czym przekazanie informacji w powyższy sposób nie zwalnia organu administracji publicznej z obowiązku ich przekazania przy pierwszej czynności skierowanej do strony (art. 122h kpa).



# Jak pracodawca oznacza obszar objęty monitoringiem wizyjnym?

Pracodawca jako administrator danych uzyskanych w toku monitoringu powinien oznaczyć obszar objęty zasięgiem kamer w sposób widoczny i czytelny. W wyniku stosowania monitoringu może bowiem dochodzić do nagrywania nie tylko pracowników, ale też osób trzecich, np. klientów przychodzących do Szkoły .

Informacje o nagrywaniu pracodawca podaje, wykorzystując w tym celu odpowiednie znaki graficzne lub ogłoszenia dźwiękowe, nie później niż dzień przed uruchomieniem monitoringu (art. 22'2 § 9 k.p.).

Może to zrobić na przykład poprzez umieszczenie w widocznych miejscach tablic zawierających stosowną klauzulę informacyjną, zgodną z art. 13 RODO.





# Zmiany w Kodeksie Pracy

## OD 25 MAJA 2018

- Art. 22'2. § 1.
- Jeżeli jest to niezbędne do zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, pracodawca może wprowadzić szczególny nadzór nad terenem zakładu pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring).
- Art. 22'3. § 1.
- Jeżeli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy, pracodawca może wprowadzić kontrolę służbowej poczty elektronicznej pracownika (monitoring poczty elektronicznej).
- § 2. Monitoring poczty elektronicznej nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika.



- § 2. Monitoring nie obejmuje pomieszczeń sanitarnych, szatni, stołówek oraz palarni, chyba że stosowanie monitoringu w tych pomieszczeniach jest niezbędne do realizacji celu określonego w § 1 i nie naruszy to godności oraz innych dóbr osobistych pracownika, w szczególności poprzez zastosowanie technik uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób. Monitoring pomieszczeń sanitarnych wymaga uzyskania uprzedniej zgody zakładowej organizacji związkowej, a jeżeli u pracodawcy nie działa zakładowa organizacja związkowa – uprzedniej zgody przedstawicieli pracowników wybranych w trybie przyjętym u danego pracodawcy.



## Prawo oświatowe

Stan prawny aktualny na dzień: 26.09.2019 Dz.U.2019.o.1148

Ustawa z dnia 14 grudnia 2016 r. -

- Art. 108a. Prawo oświatowe

- Monitoring

1. Jeżeli jest to niezbędne do zapewnienia bezpieczeństwa uczniów i pracowników lub ochrony mienia dyrektor szkoły lub placówki, w uzgodnieniu z organem prowadzącym szkołę lub placówkę oraz po przeprowadzeniu konsultacji z radą pedagogiczną, radą rodziców i samorządem uczniowskim, może wprowadzić szczególny nadzór nad pomieszczeniami szkoły lub placówki lub terenem wokół szkoły lub placówki w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring).

2. Monitoring nie powinien stanowić środka nadzoru nad jakością wykonywania pracy przez pracowników szkoły lub placówki.



**Prawo oświatowe**  
**Stan prawny aktualny na dzień: 26.09.2019 Dz.U.2019.0.1148**  
**Ustawa z dnia 14 grudnia 2016 r. - Prawo oświatowe**

- **Art. 108a. Prawo oświatowe**

- **Monitoring**

3. Monitoring nie obejmuje pomieszczeń, w których odbywają się zajęcia dydaktyczne, wychowawcze i opiekuńcze, pomieszczeń, w których uczniom jest udzielana pomoc psychologiczno-pedagogiczna, pomieszczeń przeznaczonych do odpoczynku i rekreacji pracowników, pomieszczeń sanitarnohigienicznych, gabinetu profilaktyki zdrowotnej, szatni i przebieralni, chyba że stosowanie monitoringu w tych pomieszczeniach jest niezbędne ze względu na istniejące zagrożenie dla realizacji celu określonego w ust. 1 i nie naruszy to godności oraz innych dóbr osobistych uczniów, pracowników i innych osób, w szczególności zostaną zastosowane techniki uniemożliwiające rozpoznanie przebywających w tych pomieszczeniach osób





## Prawo oświatowe

Stan prawny aktualny na dzień: 26.09.2019 Dz.U.2019.o.1148

Ustawa z dnia 14 grudnia 2016 r. - **WAŻNE**

- 4. Nagrania obrazu zawierające dane osobowe uczniów, pracowników i innych osób, których w wyniku tych nagrań można zidentyfikować, szkoła lub placówka przetwarza wyłącznie do celów, dla których zostały zebrane, i przechowuje przez okres nie dłuższy niż 3 miesiące od dnia nagrania.
- 5. Po upływie okresu, o którym mowa w ust. 4, uzyskane w wyniku monitoringu nagrania obrazu zawierające dane osobowe uczniów, pracowników i innych osób, których w wyniku tych nagrań można zidentyfikować, podlegają zniszczeniu, o ile przepisy odrębne nie stanowią inaczej.
- 6. Dyrektor szkoły lub placówki informuje uczniów i pracowników szkoły lub placówki o wprowadzeniu monitoringu, w sposób przyjęty w danej szkole lub placówce, nie później niż 14 dni przed uruchomieniem monitoringu. **WAŻNE**



## Prawo oświatowe

Stan prawny aktualny na dzień: 26.09.2019 Dz.U.2019.0.1148

Ustawa z dnia 14 grudnia 2016 r. - **WAŻNE**

- 7. Dyrektor szkoły lub placówki przed dopuszczeniem osoby do wykonywania obowiązków służbowych informuje ją na piśmie o stosowaniu monitoringu. **WAŻNE**
- 8. W przypadku wprowadzenia monitoringu dyrektor szkoły lub placówki oznacza pomieszczenia i teren monitorowany w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych, nie później niż dzień przed jego uruchomieniem.
- 9. Dyrektor szkoły lub placówki uzgadnia z organem prowadzącym szkołę lub placówkę odpowiednie środki techniczne i organizacyjne w celu ochrony przechowywanych nagrań obrazu oraz danych osobowych uczniów, pracowników i innych osób, których w wyniku tych nagrań można zidentyfikować, uzyskanych w wyniku monitoringu.



# Roczny plan kontroli sektorowych na 2019 rok UODO

- **sektor zdrowia, zatrudnienia i szkolnictwa**
- I. Szkoły i placówki oświatowe - przetwarzanie danych osobowych rejestrowanych za pomocą systemu monitoringu wizyjnego (cd. sektora rozpoczętego w IV kwartale 2018 r.).
- II. Pracodawcy - przetwarzanie danych osobowych rejestrowanych za pomocą systemu monitoringu wizyjnego. Przetwarzanie danych w związku z rekrutacją.



# UODO zawiadamia kontrolowanego o planowanej kontroli(opcjonalnie)

Organ nadzoru nie musi uprzedzać kontrolowanego o planowanej kontroli.

Niemniej jednak kontrolowany może otrzymać informację o kontroli zawierającą m.in. o terminie kontroli i jej przedmiocie





# Art. 84. Ustawy Ochr . Danych Osob .

- **Prawa kontrolującego**
- 1.Kontrolujący ma prawo:
  - 1)wstępu w godzinach od 600 do 2200 na grunt oraz do budynków, lokali lub innych pomieszczeń;
  - 2)wglądu do dokumentów i informacji mających bezpośredni związek z zakresem przedmiotowym kontroli;
  - 3)przeprowadzania oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych;
  - 4)żądać złożenia pisemnych lub ustnych wyjaśnień oraz przesłuchiwać w charakterze świadka osoby w zakresie niezbędnym do ustalenia stanu faktycznego;
  - 5)zlecać sporządzanie ekspertyz i opinii.



## Art. 84. Ustawy Ochr . Danych Osob .

- 2. Kontrolowany zapewnia kontrolującemu oraz osobom upoważnionym do udziału w kontroli warunki i środki niezbędne do sprawnego przeprowadzenia kontroli, a w szczególności sporządza we własnym zakresie kopie lub wydruki dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub systemach, o których mowa w ust. 1 pkt 3.
- 3. Kontrolowany dokonuje potwierdzenia za zgodność z oryginałem sporządzonych kopii lub wydruków, o których mowa w ust. 2. W przypadku odmowy potwierdzenia za zgodność z oryginałem kontrolujący czyni o tym wzmiankę w protokole kontroli.
- 4. W uzasadnionych przypadkach przebieg kontroli lub poszczególne czynności w jej toku, po uprzednim poinformowaniu kontrolowanego, mogą być utrwalane przy pomocy urządzeń rejestrujących obraz lub dźwięk. Informatyczne nośniki danych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2019 r. poz. 700, 730, 848 i 1590), na których zarejestrowano przebieg kontroli lub poszczególne czynności w jej toku, stanowią załącznik do protokołu kontroli.



# Przebieg kontroli

Urzędnik przeprowadzający kontrolę powinien okazać imienne upoważnienie oraz legitymację służbową. W upoważnieniu do przeprowadzenia kontroli powinny znaleźć się takie informacje jak m.in. oznaczenie kontrolowanego podmiotu oraz wskazanie daty rozpoczęcia i przewidywanego terminu zakończenia kontroli.

Na potrzeby kontroli kontrolujący ma prawo do:

- wstępu w godzinach od 6.00 do 22.00 na grunt oraz do budynków, lokali lub innych pomieszczeń;
- wglądu do wszelkich dokumentów i wszelkich informacji mających bezpośredni związek z zakresem przedmiotowym kontroli;
- przeprowadzania oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych;
- żądać złożenia pisemnych lub ustnych wyjaśnień oraz przesłuchiwać w charakterze świadka osoby w zakresie niezbędnym do ustalenia stanu faktycznego;
- zlecać sporządzanie ekspertyz i opinii.

Kontrola nie może trwać dłużej niż 30 dni od okazania kontrolowanemu upoważnienia i legitymacji służbowej lub innego dokumentu potwierdzającego tożsamość. Przebieg czynności kontrolnych kontrolujący przedstawia w protokole kontroli.



# RZECZPOSPOLITA POLSKA



Urząd Ochrony Danych Osobowych

Numer legitymacji

## LEGITYMACJA SŁUŻBOWA Pracownika

Miejsce  
na fotografię

data ważności legitymacji

(podpis wystawcy)

Miejsce  
na pieczęć

Podpis posiadacza

Nazwisko

Imię

Stanowisko służbowe





## upoważnienie do kontroli obejmowało ustalenie:

1. podstaw prawnych przetwarzania danych osobowych.
2. Zakres przetwarzania danych osobowych.
3. Cel i rodzaj przetwarzanych danych osobowych.
4. Ustalenie, czy dane osobowe są przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty (art.5 ust . 1 lit. a RODO )



## upoważnienie do kontroli obejmowało ustalenie:

5. Sposób dopełnienia obowiązków ADO wynikających z art.12,art13 ust. 1 i ust. 2 oraz art. 14 ust. 1, ust.2 i ust 3 RODO
6. Okres przetwarzania danych osobowych
7. Sposób udostępniania danych osobowych
8. Ustalenie , czy ADO wdrożył odpowiednie środki techniczne i organizacyjne, aby przetwarzanie danych osobowych odbywało się zgodnie z RODO z uwzględnieniem ryzyka naruszenia praw i wolności osób fizycznych, a także czy środki te są w razie potrzeby poddawane przeglądom i uaktualniane (art. 32, art. 24 RODO )



## upoważnienie do kontroli obejmowało ustalenie:

9. Ustalenie czy zostały wdrożone polityki i procedury ochrony danych (w tym ich formalnego obowiązywania oraz świadomości i przeszkolenia członków personelu, (art. 24 ust 2 RODO),
10. Ustalenie, czy ADO przeprowadził ocenę skutków dla ochrony danych ( art. 35 RODO)
11. Czy wyznaczono inspektora ochrony danych (art. 37 RODO)
12. Ustalenie , czy osobom dopuszczonym do przetwarzania danych osobowych zostały nadane upoważnienia do ich przetwarzania (art.29 RODO)



## upoważnienie do kontroli obejmowało ustalenie:

13. Ustalenie, czy ADO powierzył przetwarzanie danych podmiotom przetwarzającym, a jeśli tak to, czy powierzenie nastąpiło na warunkach określonych w art. 28 RODO.
14. Czy prowadzony jest rejestr czynności przetwarzania oraz rejestr wszystkich kategorii czynności przetwarzania, (art. 30 RODO)
15. Czy odpowiednio dokumentowane są przez ADO wszystkie naruszenia ochrony danych, w tym również okoliczności naruszenia, jego skutki, oraz podjęte działania zaradcze (art. 33 .ust. 5)





# 1. podstaw prawnych przetwarzania danych osobowych.(ze zmianami)

- Ustawa z dnia 26 stycznia 1982 r. Karta Nauczyciela, t.j. z dnia 13 kwietnia 2018 r. (Dz. U. z 2018 r., poz. 967).
- Rozporządzenie Ministra Edukacji Narodowej z dnia 31 października 2018 r. zmieniające rozporządzenie w sprawie bezpieczeństwa i higieny w publicznych i niepublicznych szkołach i placówkach (Dz. U. z 2018 r., poz. 2140).
- Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe, t.j. z dnia 10 maja 2018 r. (Dz. U. z 2018 r., poz. 996).
- **Kodeks Pracy**
- **Statut Placówki Oświatowej**
- **Regulamin Monitoringu jako część dokumentacji ODO**



# 1. podstaw prawnych przetwarzania danych osobowych.(ze zmianami) cd

- art. 12 i art. 13 RODO

Przepisy uszczegółowiające:

- art. 22<sup>2</sup> § 7-9 Kodeksu pracy,
- art. 108a ust. 6-8 Prawa oświatowego.
- •poinformowanie uczniów i pracowników o monitoringu, w sposób przyjęty w szkole / zakładzie pracy, 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



# Jednym z kluczowych zadań realizowanych przez szkołę jest zapewnienie uczniom bezpieczeństwa. Jakie zadania do wykonania czekają na dyrektora szkoły i nauczycieli na tej płaszczyźnie?

- Punktem wyjścia w tym zakresie są zapisy art. 6 pkt 1 oraz art. 7 ust. 2 pkt 6 Karty Nauczyciela, które stanowią, że nauczyciel jest zobowiązany do zapewnienia bezpieczeństwa uczniom w czasie zajęć organizowanych przez szkołę,
- natomiast dyrektor szkoły jest odpowiedzialny za zapewnienie bezpieczeństwa uczniom i nauczycielom w czasie zajęć organizowanych przez szkołę,
- oraz nowelizacja rozporządzenia Ministra Edukacji Narodowej w sprawie bezpieczeństwa i higieny w publicznych i niepublicznych szkołach i placówkach.



# 1. podstaw prawnych przetwarzania danych osobowych.(ze zmianami) cd

- Aby legalnie wprowadzić monitoring, pracodawca może powołać się wyłącznie na niezbędność:
- zapewnienia bezpieczeństwa pracowników, uczniów, rodziców itp
- zapewnienia ochrony mienia szkoły , parkingu itp
- Zastosowanie kamer w placówce edukacyjnej powinno znajdować uzasadnienie tylko we wskazanych wyżej przesłankach. Zgodnie z kodeksem pracy, monitoring nie może służyć np. nadzorowaniu pracy pracowników.





## 2. Zakres przetwarzania danych osobowych.

- Wizerunek ( Jasna informacja o braku nagrywania fonii )
- Czas (Okres przechowywania przez pracodawcę nagrań z monitoringu nie może przekroczyć 3 miesięcy od dnia nagrania (art. 22'2 § 3 k.p.).
- Obszar ( wewnętrzny i zewnętrzny )



### 3. Cel i rodzaj przetwarzanych danych osobowych.

- 4. Ustalenie, czy dane osobowe są przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty (art.5 ust . 1 lit. a RODO)



## 5. Sposób dopełnienia obowiązków ADO wynikających z art.12,art13 ust. 1 i ust. 2 oraz art. 14 ust. 1, ust.2 i ust 3 RODO

- Artykuł 12 – Przejrzyste informowanie i przejrzysta komunikacja oraz tryb wykonywania praw przez osobę, której dane dotyczą
- Artykuł 13 – Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą
- Artykuł 14 – Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą



## 6. Okres przetwarzania danych osobowych

- Okres przechowywania przez pracodawcę nagrań z monitoringu nie może przekroczyć 3 miesięcy od dnia nagrania (art. 22'2 § 3 k.p.).
- Jeżeli nagrania obrazu stanowią dowód w postępowaniu prowadzonym na podstawie prawa lub pracodawca otrzymał informacje, że mogą one stanowić dowód w postępowaniu, termin 3 miesięcy ulega przedłużeniu do czasu prawomocnego zakończenia postępowania (art. 22'2 § 4 k.p.).
- Po upływie dopuszczalnego prawem okresu przechowywania, uzyskane w wyniku monitoringu nagrania obrazu zawierające dane osobowe podlegają zniszczeniu, o ile przepisy odrębne nie stanowią inaczej i nie wymagają na przykład dalszego archiwizowania nagrań (art. 22'2 § 5 k.p.). (JAK NISZCZYMY ? )





## 7. Sposób udostępniania danych osobowych

- Na gruncie RODO osoba, której dane dotyczą, jest uprawniona do uzyskania od Administratora Danych Osobowych, potwierdzenia, czy przetwarza on dane osobowe jej dotyczące. Jeżeli okaże się, że ma to miejsce, wówczas osoba ta jest uprawniona do uzyskania dostępu do danych oraz następujących informacji:



## 7. Sposób udostępniania danych osobowych

- Na gruncie RODO osoba, której dane dotyczą, jest uprawniona do uzyskania od Administratora Danych Osobowych, potwierdzenia, czy przetwarza on dane osobowe jej dotyczące. Jeżeli okaże się, że ma to miejsce, wówczas osoba ta jest uprawniona do uzyskania dostępu do danych oraz następujących informacji:
- **udostępnienie danych na podstawie art. 15 ust. 3 RODO odbywa się - w przypadku pierwszej kopii danych – bezpłatnie**
- **Jak udostępniamy :Policji , Straży Miejskiej , Prokuraturze ?**
- **WNIOSEK O UDOSTĘPNIENIE – WZÓR W DOKUMENTACJI ODO**

- 8. Ustalenie , czy ADO wdrożył odpowiednie środki techniczne i organizacyjne, aby przetwarzanie danych osobowych odbywało się zgodnie z RODO z uwzględnieniem ryzyka naruszenia praw i wolności osób fizycznych, a także czy środki te są w razie potrzeby poddawane przeglądom i uaktualniane (art. 32, art. 24 RODO )

# „Monitoring sąsiadów”

**9. Ustalenie czy zostały wdrożone polityki i procedury ochrony danych (w tym ich formalnego obowiązywania oraz świadomości i przeszkolenia członków personelu, (art. 24 ust 2 RODO),**

- Karty szkolenia wstępnego
- Karty szkoleń okresowych
- Tematyka szkoleń (czy obejmowała monitoring wizyjny)
- Listy obecności czy jest podpisana przez pracowników i z jaka datą
- Certyfikaty ze szkoleń w teczkach akt osobowych
- Dokumentacja – Polityki instrukcje , Regulamin monitoringu
- Dokumentacja – procedury w przypadku wystąpienia incydentu
- Rejestr Incydentów





## 10. Ustalenie, czy ADO przeprowadził ocenę skutków dla ochrony danych ( art. 35 RODO)

- Monitoring wizyjny jest bez wątpienia procesem przetwarzania danych osobowych, takich jak wizerunek osoby. **Zgodnie z art. 35 RODO** administrator przed rozpoczęciem operacji przetwarzania danych jest zobowiązany do dokonania oceny skutków przetwarzania dla ochrony danych. Administrator powinien przeprowadzić taką ocenę w przypadku, w którym dany rodzaj przetwarzania ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.



## **10. Ustalenie, czy ADO przeprowadził ocenę skutków dla ochrony danych ( art. 35 RODO)**

- 24 sierpnia 2018 r. został ogłoszony w Monitorze Polskim pierwszy Komunikat Prezesa Urzędu Ochrony Danych Osobowych (dalej także jako PUODO) z dnia 17 sierpnia 2018 r.
- W komunikacie zostały wskazane operacje przetwarzania, które wymagają od administratora przeprowadzenia oceny skutków przetwarzania danych osobowych w ramach konkretnych kategorii danych osobowych przetwarzanych w podmiocie.
- Katalog przypadków, kiedy obowiązkowo trzeba stosować ocenę skutków jest katalogiem zamkniętym.



# Jak powinno wyglądać dokonywanie oceny skutków przetwarzania w praktyce?

- Zgodnie z art. 35 ust. 7 RODO ocena skutków przetwarzania powinna zawierać co najmniej:
- systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
- ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
- ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
- środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa, mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.



## Administrator może przeprowadzać oceny skutków przetwarzania w oderwaniu od całego systemu ochrony danych osobowych

- konsultować dokonywanie oceny z inspektorem ochrony danych, jeżeli takiego powołał (art. 35 ust. 2 RODO);
- w stosownych przypadkach zasięgnąć również opinii osób, których dane dotyczą, lub ich przedstawicieli w sprawie zamierzonego przetwarzania, bez uszczerbku dla ochrony interesów handlowych lub publicznych lub bezpieczeństwa operacji przetwarzania (art. 35 ust. 9 RODO);
- dokonywać przeglądu – w razie zmiany ryzyka wynikającego z danej operacji przetwarzania, stwierdzić, czy przetwarzanie odbywa się zgodnie z dotychczasową oceną skutków dla ochrony danych (art. 35 ust. 11 RODO).





## Ocena ryzyka

Na etapie oceny ryzyka określa się, które ryzyka są akceptowalne poprzez porównanie wyznaczonych poziomów ryzyk z ryzykiem, które można zaakceptować. W przypadku gdy ryzyka są większe od ryzyka akceptowalnego wprowadza się działania zaradcze (proces postępowania z ryzykiem). Dla ryzyk, które nie mogą być zaakceptowane ze względu na ich zbyt wysoki poziom, proces postępowania z ryzykiem przeprowadza się ponownie. Ryzyka pozostające po procesie postępowania z ryzykiem (ryzyka szczątkowe) podlegają procesowi akceptacji ryzyka.

Ryzyka naruszenia bezpieczeństwa zostały posortowane od największego do najmniejszego. Poniżej przedstawiono 500 największych wartości w tablicy oceny ryzyka dla poufności, dostępności i integralności.

### Ryzyko akceptowalne: 4

| POUFNOŚĆ                                                           |                                                               |        |     |
|--------------------------------------------------------------------|---------------------------------------------------------------|--------|-----|
| AKTYWA                                                             | ZAGROŻENIA                                                    | RYZYKO | AKC |
| Dane osobowe - szczególne kategorie na przenośnym nośniku pamięci  | Złośliwe oprogramowanie (umyślne)                             | 3.6    | TAK |
| Dane osobowe - szczególne kategorie w postaci wydruków na papierze | Kradzież dokumentów (umyślne)                                 | 3.2    | TAK |
| Hosting danych osobowych                                           | Manipulacja konfiguracją (umyślne)                            | 3.2    | TAK |
| Hosting danych osobowych                                           | Ujawnienie (umyślne)                                          | 3.0    | TAK |
| Oprogramowanie do inspekcji sieci IDS/IPS                          | Złośliwe oprogramowanie (umyślne)                             | 3.0    | TAK |
| Dane osobowe na przenośnym nośniku pamięci                         | Złośliwe oprogramowanie (umyślne)                             | 2.8    | TAK |
| Dane osobowe - szczególne kategorie w postaci wydruków na papierze | Ujawnienie (przypadkowe)                                      | 2.7    | TAK |
| Hosting danych osobowych                                           | Szpiegostwo zdalne (umyślne)                                  | 2.7    | TAK |
| Drukarka                                                           | Użycie nielegalnego lub skopiowanego oprogramowania (umyślne) | 2.7    | TAK |
| Drukarka sieciowa                                                  | Użycie nielegalnego lub skopiowanego oprogramowania (umyślne) | 2.7    | TAK |
| Dane osobowe - szczególne kategorie na przenośnym nośniku pamięci  | Sfałszowanie oprogramowania (umyślne)                         | 2.6    | TAK |



| DOSTĘPNOŚĆ                                                         |                                                               |       |     |
|--------------------------------------------------------------------|---------------------------------------------------------------|-------|-----|
| AKTYWA                                                             | ZAGROŻENIA                                                    | RYZYO | AKC |
| Dysk twardy                                                        | Skasowanie informacji (umyślne)                               | 5.0   | NIE |
| Hosting danych osobowych                                           | Manipulacja konfiguracją (umyślne)                            | 4.6   | NIE |
| Drukarka                                                           | Użycie nielegalnego lub skopiowanego oprogramowania (umyślne) | 4.4   | NIE |
| Drukarka sieciowa                                                  | Użycie nielegalnego lub skopiowanego oprogramowania (umyślne) | 4.4   | NIE |
| Płyta CD/DVD                                                       | Pożar (umyślne)                                               | 4.4   | NIE |
| Oprogramowanie do inspekcji sieci IDS/IPS                          | Złośliwe oprogramowanie (umyślne)                             | 4.2   | NIE |
| Dane osobowe na przenośnym nośniku pamięci                         | Manipulacja urządzeniem (umyślne)                             | 4.1   | NIE |
| Dane osobowe na płycie CD/DVD                                      | Manipulacja urządzeniem (umyślne)                             | 4.1   | NIE |
| Dane osobowe - szczególne kategorie na przenośnym nośniku pamięci  | Manipulacja urządzeniem (umyślne)                             | 4.1   | NIE |
| Dane osobowe - szczególne kategorie na płycie CD/DVD               | Manipulacja urządzeniem (umyślne)                             | 4.1   | NIE |
| Pamięć FLASH (pendrive)                                            | Manipulacja urządzeniem (umyślne)                             | 4.1   | NIE |
| Płyta CD/DVD                                                       | Manipulacja urządzeniem (umyślne)                             | 4.1   | NIE |
| Dane osobowe na przenośnym nośniku pamięci                         | Złośliwe oprogramowanie (umyślne)                             | 4.0   | TAK |
| Dane osobowe - szczególne kategorie na przenośnym nośniku pamięci  | Złośliwe oprogramowanie (umyślne)                             | 4.0   | TAK |
| Hosting danych osobowych                                           | Przerwy w łączności, transmisji danych (umyślne)              | 3.9   | TAK |
| Automatyczne systemy bilingowe                                     | Awaria systemu klimatyzacji (umyślne)                         | 3.9   | TAK |
| Automatyczne systemy bankowe                                       | Awaria systemu klimatyzacji (umyślne)                         | 3.9   | TAK |
| Serwer                                                             | Awaria systemu klimatyzacji (umyślne)                         | 3.9   | TAK |
| E-mail                                                             | Awaria łączności (przypadkowe)                                | 3.8   | TAK |
| WWW                                                                | Awaria łączności (przypadkowe)                                | 3.8   | TAK |
| Zdalny dostęp                                                      | Awaria łączności (przypadkowe)                                | 3.8   | TAK |
| Urządzenie wielofunkcyjne (drukarka, skaner, ksero)                | Użycie nielegalnego lub skopiowanego oprogramowania (umyślne) | 3.8   | TAK |
| Komputer PC                                                        | Zniszczenie nośników (umyślne)                                | 3.7   | TAK |
| Serwer                                                             | Zniszczenie nośników (umyślne)                                | 3.7   | TAK |
| Drukarka                                                           | Sfałszowanie oprogramowania (umyślne)                         | 3.7   | TAK |
| Drukarka sieciowa                                                  | Sfałszowanie oprogramowania (umyślne)                         | 3.7   | TAK |
| Urządzenie wielofunkcyjne (drukarka, skaner, ksero)                | Sfałszowanie oprogramowania (umyślne)                         | 3.7   | TAK |
| Zasilanie energetyczne                                             | Manipulacja konfiguracją (umyślne)                            | 3.7   | TAK |
| Dane osobowe w postaci wydruków na papierze                        | Kradzież dokumentów (umyślne)                                 | 3.6   | TAK |
| Dane osobowe - szczególne kategorie w postaci wydruków na papierze | Kradzież dokumentów (umyślne)                                 | 3.6   | TAK |

# Ważne

- **UODO SPRAWDZA:**
- Czy monitoring jest podłączony do Internetu (jeżeli tak to kto ma do niego dostęp i jakie są zabezpieczenia)
- Czy są to sieci wydzielone
- Czy osoby postronne mogą oglądać obraz
- Czy są atrapy kamer
- Jak często zmieniane są hasła do rejestratorów
- **UODO nie zaleca podłączania monitoringu do Internetu w Szkołach oraz montaż atrap kamer**



# 11. Czy wyznaczono inspektora ochrony danych (art. 37 RODO)

- **Oświadczenie o braku konfliktu interesów:**

RODO w art. 38 ust. 6 daje IOD możliwość wykonywania innych zadań i obowiązków niż te, które zostały określone w art. 37 RODO. Obowiązki te jednak nie mogą prowadzić do konfliktu interesów.

Konflikt interesów to sytuacja, w której IOD zajmowałby stanowisko, umożliwiające mu określanie sposobów i celów przetwarzania danych co mogłoby wykluczać jego niezależność, a także wymagać stawiania celów biznesowych ponad prawa i wolności podmiotu danych.

**Przykład : Czy pracownik administracyjny szkoły lub nauczyciel jako IOD sam siebie kontroluje obiektywnie ? I przedstawi to w raporcie Dyrektorowi Szkoły .**



# 11. Czy wyznaczono inspektora ochrony danych (art. 37 RODO) cd

- Zgłoszenie IOD do UODO (wraz z zastępcami jeżeli powołano)

PONAD TO DOSTARCZYLIŚMY URZĘDNIKOM UODO:

- Dyplomy potwierdzające , kwalifikacje zawodowe do pełnienia funkcji IOD oraz zastępców IOD (kserokopie dyplomów ukończonych studiów)
- Certyfikaty Audytorów Wewnętrznych Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001 – 2017 (kserokopia)
- oraz Dedykowane polisy OC dla IOD (kserokopia)





## 12. Ustalenie , czy osobom dopuszczonym do przetwarzania danych osobowych zostały nadane upoważnienia do ich przetwarzania (art.29 RODO)

- Dedykowane upoważnienia do przetwarzania danych osobowych w monitoringu wizyjnym.
- Dedykowane loginy i hasła do rejestratora monitoringu dla pracowników upoważnionych - jak często są zmieniane
- Rejestr upoważnień

*Częsty błąd w upoważnieniach: Upoważnienie obejmuje zakres przetwarzania danych zgodny umową o pracę / zakres obowiązków :*

*Np.: Sprzątaczką, woźną, konserwator, portier itp*



**13. Ustalenie, czy ADO powierzył przetwarzanie danych podmiotom przetwarzającym, a jeśli tak to, czy powierzenie nastąpiło na warunkach określonych w art. 28 RODO.**

- Umowy powierzenia danych (jaka jest treść) np.:
- z agencją ochrony
- serwisem monitoringu  
(czy prowadzona jest książka serwisowa)
- Administratorem budynku



**14. Czy prowadzony jest rejestr czynności przetwarzania oraz rejestr wszystkich kategorii czynności przetwarzania, ( art. 30 RODO)**

**15. Czy odpowiednio dokumentowane są przez ADO wszystkie naruszenia ochrony danych , w tym również okoliczności naruszenia, jego skutki , oraz podjęte działania zaradcze (art . 33 .ust. 5)**



# Sankcje

Organ nadzorczy ma również szereg uprawnień naprawczych (zgodnie z art. 58 ust. 2 RODO). Są to w szczególności:

- wydawanie ostrzeżeń administratorowi lub podmiotowi przetwarzającemu dotyczących możliwości naruszenia RODO poprzez planowane operacje przetwarzania;
- udzielanie upomnień administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia RODO przez operacje przetwarzania;
- nakazanie administratorowi lub podmiotowi przetwarzającemu spełnienia żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej;
- nakazanie administratorowi lub podmiotowi przetwarzającemu dostosowania operacji przetwarzania do RODO, a w stosownych przypadkach wskazanie sposobu i terminu;
- nakazanie administratorowi zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych;
- wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania;
- nakazanie sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania oraz nakazanie powiadomienia o tych czynnościach odbiorców, którym dane osobowe ujawniono;
- zastosowanie, oprócz lub zamiast środków naprawczych, administracyjnej kary pieniężnej, zależnie od okoliczności konkretnej sprawy.





**Dziękuję za uwagę Tomasz Paprocki FUSION 24**  
**Agencja Bezpieczeństwa Informacji**  
**biuro@abifusion24.pl**  
**735 008 215/16**

