
# Wskazówki

# Prezesa Urzędu Ochrony Danych Osobowych

# dotyczące wykorzystywania monitoringu wizyjnego

Wersja 1
czerwiec 2018

# Spis treści

# I. Wprowadzenie

Monitoring wizyjny jest inwazyjną formą przetwarzania danych osobowych i jako taki powinien podlegać szczególnej weryfikacji przez administratora potrzeby jego stosowania i konieczności zabezpieczenia oraz kontroli przez organy kontrolne.

**Nową, uchwaloną 10 maja 2018 r., ustawą o ochronie danych osobowych[1] znowelizowano przepisy sektorowe dotyczące monitoringu wizyjnego stosowanego przez pracodawców, placówki oświatowe oraz jednostki samorządu terytorialnego.** Weszły one w życie 25 maja 2018 r., a więc w dniu rozpoczęcia stosowania ogólnego rozporządzenia o ochronie danych, czyli RODO[2]. Ustawodawca nie przewidział w tym przypadku szczególnych okresów przejściowych na dostosowanie się do nowych regulacji. Tymczasem u administratorów zrodziły one wiele wątpliwości interpretacyjnych i obawy o możliwość nałożenia przez Prezesa Urzędu Ochrony Danych Osobowych kar finansowych za niespełnienie ciążących na nich obowiązków. Dodatkowo administratorzy reprezentujący inne sektory i branże, dla których w przepisach sektorowych nie określono zasad prowadzenia monitoringu, mają wątpliwości co do podstaw prawnych prowadzenia systemów wideonadzoru.

W celu rozwiania tych wątpliwości Prezes Urzędu przygotował niniejsze wskazówki. Dotyczą one monitoringu wizyjnego stosowanego zgodnie z przepisami rozporządzenia 2016/679. **Wskazówki dla sektorów policyjnego i sądowego, które podlegają przepisom dyrektywy 2016/680[3], mogą być wydane po przyjęciu przepisów wdrażających dyrektywę do polskiego porządku prawnego.[4]**

---

[1] ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000, **dalej zwanej ustawą lub u.o.d.o.**).

[2] Rozporządzenie Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenia o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2), **dalej zwane także rozporządzeniem lub RODO.**

[3] dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 04.05.2016, str. 89 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 10), **dalej zwaną także dyrektywą lub DODO.**

[4] Projekt ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, obecnie procedowany przez Komitet do Spraw Europejskich: http://legislacja.rcl.gov.pl/docs//2/12310605/12502714/12502715/dokument343349.pdf

Zgodnie z art. 34 ust. 1 i 2 u.o.d.o. Prezes Urzędu jest organem właściwym w sprawie ochrony danych osobowych oraz organem nadzorczym w rozumieniu:

1) rozporządzenia 2016/679,
2) dyrektywy 2016/680 oraz
3) rozporządzenia 2016/794[5].

**Niniejszy dokument został przygotowany na podstawie art. 57 ust. 1 lit. d rozporządzenia 2016/679 jako materiał edukacyjny.** Wiążąca ocena prawidłowości operacji przetwarzania danych osobowych, jaką jest stosowanie monitoringu wizyjnego, jest każdorazowo prowadzona przez Prezesa Urzędu w trybie właściwych postępowań, o których mowa w art. 57 ust. 1 lit. a i f rozporządzenia, tj. w ramach kontroli monitorowania i egzekwowania przepisów o ochronie danych albo ze skargi na przetwarzanie danych osobowych.

**Zważywszy wątpliwości związane z nowymi przepisami oraz zróżnicowanym charakterem stosowanych obecnie systemów monitoringu wizyjnego Prezes Urzędu Ochrony Danych Osobowych zachęca do udziału w konsultacjach niniejszego dokumentu.** Mają one na celu jak najdokładniejsze poznanie potrzeb i opinii różnych środowisk w tej sprawie. **Wszystkie zainteresowane osoby, w szczególności zrzeszenia branżowe i organizacje pozarządowe, mogą przedstawić swoje stanowisko. Uwagi do poszczególnych punktów i sugestie co do nieporuszonych kwestii, które Państwa zdaniem powinny zostać poruszone należy przesyłać do 15 lipca 2018 r. na adres: DESiWM@uodo.gov.pl. W tytule wiadomości prosimy wskazać hasło „Konsultacje Monitoring". Wynikiem konsultacji będzie publikacja ostatecznej wersji wskazówek.**

[5] rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępującego i uchylającego decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW (Dz. Urz. UE L 135 z 24.05.2016, str. 53).

# II. Informacje ogólne

## 1. Obowiązujące przepisy

Stosowanie monitoringu wizyjnego jako formy nadzoru nad osobami, których dane dotyczą, wiąże się z przetwarzaniem danych osobowych wszystkich obserwowanych osób. W polskim porządku prawnym, mimo zabiegów m.in. Rzecznika Praw Obywatelskich oraz Generalnego Inspektora Ochrony Danych Osobowych, nie funkcjonowała dotąd regulacja ogólna tego zagadnienia. Prowadzone prace legislacyjne miały przerwać ten stan, jednak nie wyszły poza prace koncepcyjne. Z tego powodu do oceny spraw związanych z monitoringiem wizyjnym stosowano w odpowiednim zakresie przepisy ustawy o ochronie danych osobowych obowiązującej do 25 maja 2018 r.

Istniejące (wskazane poniżej) i projektowane[1] regulacje monitoringu dotyczą różnych sektorów i osób. W zakresie nieuregulowanym w takich przepisach konieczne jest stosowanie przepisów ogólnych o ochronie danych. Ma to np. znaczenie w przypadku monitoringu w zakładzie pracy, gdzie przepisy zezwalają na obserwowanie jedynie osób zatrudnionych, a nie odnoszą się do osób odwiedzających teren (klienci, dostawcy, osoby prowadzące kontrole itp.).

Wszystkie te procesy podlegają rygorom rozporządzenia 2016/679 (które bezpośrednio w art. 35 wspomina o systematycznym monitorowaniu na dużą skalę miejsc dostępnych publicznie), u.o.d.o. oraz ustaw szczególnych i aktów wykonawczych. Regulują one uprawnienia i obowiązki podmiotów mogących prowadzić obserwację przede wszystkim miejsc publicznych, osób i mienia w celu zapewniania bezpieczeństwa. Wśród nich w szczególności wymienić należy przepisy dot. sektorów:

a) publicznego:
   1) Art. 9a ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2018 r. poz. 994 i 1000);
   2) Art. 4b ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2018 r. poz. 995 i 1000);
   3) Art. 60a ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa (Dz. U. z 2018 r. poz. 913);
   4) Art. 5a ustawy z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym (Dz. U. poz. 2259 z późn. zm.);
b) prywatnego:

[1] M.in. art. 4, 25 i 166 projektu ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679, http://legislacja.rcl.gov.pl/projekt/12302951/katalog/12457732#12457732

1) Art. 15b ustawy z dnia 19 listopada 2009 r. o grach hazardowych (Dz. U. z 2018 r. poz. 165 z późn. zm.).
2) Art. 11 ustawy z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych (Dz. U. z 2017 r. poz. 1160 z późn. zm.).

c) zdrowia, zatrudnienia i szkolnictwa:
1) Art. $22^2$ ustawy z dnia 26 czerwca 1974 r. - Kodeks pracy (Dz. U. z 2018 r. poz. 917 i 1000);
2) Art. 108a ustawy z dnia 14 grudnia 2016 r. - Prawo oświatowe (Dz. U. z 2018 r. poz. 996 i 1000);
3) Art. 43e ustawy z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (Dz. U. z 2017 r. poz. 882 z późn. zm.)
4) Art. 22 ust. 3 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz. U. z 2018 r. poz. 160 z późn. zm.).

d) organów ścigania i sądów:
1) Art. 15 i 19 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2017 r. poz. 2067 z późn. zm.);
2) Art. 20g ustawy z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z 2017 r. poz. 2222 z późn. zm.);
3) Art. 157 ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (Dz. U. z 2018 r. poz. 155 z późn. zm.);
4) Art. 147 ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. z 2017 r. poz. 1904 z późn. zm.).

**Należy jednocześnie mieć na uwadze, że były one przyjmowane przez wiele lat i nie muszą zawierać kompletnej regulacji omawianej formy nadzoru. W takich przypadkach zastosowanie będą miały przepisy rozporządzenia 2016/679 lub dyrektywy 2016/680[2].**

Uchwalone w nowej ustawie o ochronie danych osobowych przepisy szczególne dotyczące monitoringu wizyjnego nie przewidują okresów przejściowych, na które nie zdecydował się ustawodawca. Także przepisy RODO nie przewidują dodatkowych terminów na dostosowanie. **W związku z tym Prezes Urzędu przyjmuje, że przepisy te oraz właściwe postanowienia RODO mają zastosowanie do wszystkich istniejących i przyszłych systemów nadzoru wizualnego.** Jednocześnie organ nadzorczy zdaje sobie sprawę, że przystosowanie systemów do nowych przepisów wymaga przeprowadzenia konsultacji z

[2] Do czasu przyjęcia ustawy wdrażającej zastosowanie ma art. 175 ustawy, zgodnie z którym stosuje się wybrane przepisy dotychczasowej ustawy o ochronie danych osobowych.

zaangażowanymi podmiotami, zmian dokumentów wewnętrznych oraz spełnienia obowiązków wobec osób obserwowanych. **Dlatego organ ds. ochrony danych osobowych będzie w pierwszej kolejności monitorował postępy w dostosowywaniu do nowych wymogów. Działania takie powinny być przez administratorów i podmioty przetwarzające podejmowane niezwłocznie, tak by wykazać dążenie do zapewnienia zgodności z obowiązującym prawem. W dalszej kolejności prowadzone będą działania weryfikujące wypełnianie zasad stosowania monitoringu wizyjnego przewidzianych w RODO oraz przepisach szczególnych.**

## 2. Ważne definicje

Każdy ma prawo do ochrony dotyczących go danych osobowych. Rozporządzenie wprowadza normy służące realizacji tego prawa. W szczególności reguluje następujące definicje:

**2.1.** dane osobowe – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą").

Należy pamiętać, że możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie: imienia i nazwiska, numeru identyfikacyjnego, danych o lokalizacji, identyfikatora internetowego lub jednego bądź kilku szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Danymi osobowymi nie będą jednak pojedyncze informacje o dużym stopniu ogólności. Staną się nimi dopiero z chwilą zestawienia ich z innymi, dodatkowymi informacjami, które w konsekwencji pozwolą na odniesienie ich do konkretnej osoby. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

<u>Na podstawie przepisów rozporządzenia wyróżnić można:</u>

a) dane tzw. zwykłe, takie jak np. imię, nazwisko, adres zamieszkania, data i miejsce urodzenia, numer telefonu, wykonywany zawód, wizerunek itp.
b) szczególne kategorie danych osobowych (tzw. dane wrażliwe), wymienione w art. 9 i 10 rozporządzenia dane ujawniające:
    - pochodzenie rasowe lub etniczne,
    - poglądy polityczne,
    - przekonania religijne lub światopoglądowe,
    - przynależność do związków zawodowych,

- dane genetyczne,
- dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej,
- dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby,
- dane dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa.

Należy mieć na uwadze, że przetwarzanie szczególnych kategorii danych wiąże się z koniecznością wypełnienia dodatkowych gwarancji ich ochrony ujętych w art. 9 ust. 2 i art. 10 RODO oraz szczegółowych przepisach krajowych.

Zgodnie z wyrokiem w sprawie C-434/16[3] pojęcie danych osobowych obejmuje także pisemne odpowiedzi udzielone przez osobę przystępującą do egzaminu zawodowego i ewentualne naniesione przez egzaminatora komentarze odnoszące się do tych odpowiedzi. **Oznacza to, że dane osobowe nie muszą pochodzić jedynie od osoby, której dane dotyczą.**

**Odnosząc się do zakresu danych osobowych przetwarzanych przez monitoring wizyjny właściwym jest wskazywanie w szczególności** wizerunków, cech szczególnych osób i numerów identyfikacyjnych (np. numery tablic rejestracyjnych i numerów bocznych pojazdów).

**2.2. przetwarzanie –** operacja 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.

**W przypadku monitoringu wizyjnego będą to operacje polegające w szczególności na zapisywaniu, przeglądaniu, udostępnianiu i usuwaniu nagrań zarejestrowanych zdarzeń i osób niezależnie od charakteru nośnika, w którym są przechowywane (dyski twarde systemu, nagrania zapisane w pamięci urządzenia umożliwiającego zdalny dostęp – smartfon, komputery przenośne itp.).**

3 Wyrok Trybunału Sprawiedliwości z dnia 20 grudnia 2017 r. w sprawie C-434/16 Peter Nowak przeciwko Data Protection Commissioner

# 3. Podstawy i zasady stosowania monitoringu wizyjnego

## 3.1. Podstawy przetwarzania danych osobowych

Rozporządzenie 2016/679 określa zasady przetwarzania danych osobowych oraz podstawy umożliwiające ich przetwarzanie.

**Przetwarzanie danych zwykłych może się odbywać jedynie po spełnieniu jednego z warunków określonych w art. 6, a w przypadku danych wrażliwych w art. 9 i 10 rozporządzenia.**

Podstawą przetwarzania danych zwykłych może być:

a) zgoda osoby, której dane dotyczą na przetwarzanie w jednym lub większej liczbie określonych celów;
b) wykonanie umowy, której stroną jest osoba, której dane dotyczą lub podjęcie działań na żądanie takiej osoby przed zawarciem umowy;
c) wypełnienie obowiązku prawnego ciążącego na administratorze;
d) ochrona żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
e) wykonanie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
f) cele wynikające 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.

Ostatnia z wymienionych podstaw nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań. Oznacza to, że tylko podmioty prywatne mogą się powoływać na tę przesłankę, chyba że uczestniczą w realizacji zadań publicznych. **Tym samym organy publiczne, które w celu wykonywania swoich zadań korzystają z monitoringu wizyjnego, muszą opierać się na przepisach dopuszczających albo nakazujących taką formę wykonywania ich zadań.**

**Z powyższego jasno wynika, że najbardziej odpowiadającymi stosowaniu monitoringu wizyjnego przesłankami są wypełnienie obowiązku prawnego ciążącego na administratorze, wykonanie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi oraz cele wynikające z prawnie uzasadnionych interesów realizowanych przez administratora, odpowiednio dla podmiotów sektora publicznego i sektora prywatnego.**

**Przetwarzanie szczególnych kategorii danych osobowych, co do zasady, jest zabronione z wyjątkiem sytuacji określonych w art. 9 ust. 2 i art. 10 rozporządzenia.** Zgodnie z motywem 51 RODO, przetwarzanie fotografii nie powinno zawsze stanowić przetwarzania szczególnych kategorii danych osobowych, gdyż fotografie są objęte definicją "danych biometrycznych" tylko w przypadkach, gdy są przetwarzane specjalnymi metodami technicznymi, umożliwiającymi jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości. Takich danych osobowych nie należy przetwarzać, chyba że rozporządzenie dopuszcza ich przetwarzanie w szczególnych przypadkach, przy czym należy uwzględnić, że prawo państw członkowskich może obejmować przepisy szczegółowe o ochronie danych dostosowujące zastosowanie przepisów rozporządzenia tak, by można było wypełnić obowiązki prawne lub wykonać zadanie realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. **Mając na uwadze, że nagrania mogą być analizowane klatka po klatce obrazu i przy użyciu specjalnych metod technicznych (automatyczna analiza obrazu) wykorzystane do identyfikacji osób obserwowanych, tylko takie systemy monitorowania będą przetwarzały dane biometryczne w rozumieniu art. 9 ust. 1 RODO. Tego typu operacje wymagać będą wyczerpujących podstaw prawnych oraz wypełnienia dodatkowych obowiązków związanych z przetwarzaniem szczególnych kategorii danych osobowych.** Obejmuje to w szczególności dokonanie oceny skutków dla ochrony danych na podstawie art. 35 ust. 3 lit. b RODO obok wymaganej dla systemów monitoringu oceny na podstawie lit. c tego samego przepisu.

Prezes Urzędu przygotował **propozycję wykazu rodzajów przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków dla ochrony danych**[4]**.** W ostatecznej wersji dokumentu wskazano, jakie operacje przetwarzania przy użyciu monitoringu wizyjnego wymagają przeprowadzenia oceny skutków. Są to:

1) **Systematyczne monitorowanie na dużą skale miejsc dostępnych publicznie wykorzystujące elementy rozpoznawania cech lub właściwości obiektów, które znajda się w monitorowanej przestrzeni. Do tej grupy systemów nie są zaliczane systemy monitoringu wizyjnego, w których obraz jest nagrywany i wykorzystywany tylko w przypadku potrzeby analizy incydentów naruszenia prawa.**

| | |
|---|---|
| Rozbudowane systemy monitoringu przestrzeni publicznej umożliwiające śledzenie osób i | Środki komunikacji miejskiej, miasta oferujące systemy wypożyczania rowerów, |

[4] https://giodo.gov.pl/pl/1520281/10430; https://uodo.gov.pl/pl/123/212

| | |
|---|---|
| pozyskiwanie danych wykraczających poza dane niezbędne do świadczenia usługi. | samochodów oraz wyznaczające strefy płatnego parkowania. |

2) **Zautomatyzowane podejmowanie decyzji <u>wywołujących skutki prawne, finansowe lub podobne istotne skutki.</u>**

| | |
|---|---|
| Systemy monitoringu wykorzystywane do zarządzania ruchem lub przeciwdziałania zagrożeniom/nadużyciom drogowym, umożliwiające szczegółowy nadzór nad każdym kierowcą oraz jego zachowaniem na drodze w szczególności systemy pozwalające na automatyczną identyfikację pojazdów. | Drogi objęte odcinkowym pomiarem prędkości (system gromadzi informacje nie tylko o pojazdach naruszających przepisy, ale o wszystkich pojazdach pojawiających się w kontrolowanym obszarze*)*, odcinki dróg wyposażone w system elektronicznego poboru opłat viaTOLL. |

### 3.2. Zasady przetwarzania danych osobowych

Główne zasady postępowania przy przetwarzaniu danych osobowych wyznacza art. 5 ust. 1 RODO, ujmując je w formę podstawowych obowiązków administratora. Z jego treści wynika, że dane osobowe muszą być:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (**zgodność z prawem, rzetelność i przejrzystość**);
b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (**ograniczenie celu**);
c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (**minimalizacja danych**);
d) prawidłowe i w razie potrzeby uaktualniane, a dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, muszą być niezwłocznie usunięte lub sprostowane (**prawidłowość**);
e) przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane (**ograniczenie przechowywania**);
f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową

utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (**integralność i poufność**).

Zgodnie z ust. 2 omawianego przepisu, administrator jest odpowiedzialny za przestrzeganie powyższych zasad i musi być w stanie wykazać ich przestrzeganie (**rozliczalność**).

# 4. Uczestnicy procesu przetwarzania

## 4.1. Osoba, której dane dotyczą – osoba obserwowana

Zidentyfikowana lub możliwa do zidentyfikowania osoba fizyczna, której dane zostaną zebrane poprzez system monitoringu wizyjnego, może korzystać z praw ujętych w rozdziale III rozporządzenia. **Mając na uwadze specyfikę wideomonitoringu, należy stwierdzić, że realizacja uprawnień kontrolnych osoby obserwowanej może się związać z koniecznością przedstawienia przez nią informacji o sytuacjach, w których mogła znaleźć się w obszarze działania systemu monitoringu.** Może to obejmować okresy czasu czy też sytuacje, w których uczestniczyła taka osoba, szczegóły jej ubioru itp. Zgodnie z ostatnim zdaniem motywu 63, jeżeli administrator przetwarza duże ilości informacji o osobie, której dane dotyczą, powinien on mieć możliwość zażądania, przed podaniem informacji, by osoba, której dane dotyczą, sprecyzowała informacje lub czynności przetwarzania, których dotyczy jej żądanie. Jeżeli przepisy szczególne nie stanowią inaczej, odpowiedź na zapytania osoby obserwowanej powinna zostać udzielona bez zbędnej zwłoki, najpóźniej w ciągu miesiąca.

## 4.2. Administrator

Realizacja zasad przetwarzania danych osobowych należy do obowiązków **administratora**, którym zgodnie z art. 4 pkt 7 rozporządzenia jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. O tym, kto jest administratorem danych w sektorze publicznym, mogą rozstrzygać przepisy szczególne.

Administratorem danych osób obserwowanych (**operator systemu monitoringu**) jest podmiot, który podejmuje decyzje o instalacji, celach i obszarze objętym systemem monitoringu będącym w jego dyspozycji. Może on działać przez osoby kierujące i reprezentujące go na zewnątrz, jak np. zarząd spółki, dyrektor szkoły itd. Funkcjonariusze ci **zobowiązani są zapewnić w kierowanej przez siebie jednostce**

**organizacyjnej zgodne z prawem przetwarzanie danych osobowych oraz ponoszą odpowiedzialność za działania wszystkich osób upoważnionych do przetwarzania danych.**

Administrator, podejmując decyzję o stosowaniu tej formy nadzoru, powinien zweryfikować, czy realizowane przez niego cele uzasadniają obserwację osób. Administrator powinien mieć w świadomości zasadę ograniczenia celu z art. 5 ust. 1 lit. b RODO. Musi więc brać pod uwagę potrzebę ochrony prawa do prywatności i ochrony danych osobowych i ich ograniczanie tylko w niezbędnym zakresie. Oznacza to, że monitoring może być wprowadzany wtedy, kiedy inne, mniej inwazyjne metody zapewniania bezpieczeństwa są niewystarczające. Przykładowo kamery mogą być zbędne, jeżeli obszar holów szkolnych jest obserwowany przez dyżurujących nauczycieli czy teren szkoły po jej zamknięciu jest monitorowany przez dozorcę albo pracowników ochrony. Właściwym postępowaniem jest też angażowanie w proces decyzyjny dotyczący stosowania monitoringu przedstawicieli osób obserwowanych. Obecnie przewidują to powoływane już przepisy Kodeksu pracy i Prawa oświatowego, w których wskazano na konieczność prowadzenia konsultacji z pracownikami czy organem prowadzącym oraz społecznością szkolną.

Podejmując decyzję o wprowadzeniu monitoringu, administrator musi pamiętać o przeprowadzeniu **oceny skutków dla ochrony danych**. Jest ona wymagana, gdy operacja przetwarzania ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Zgodnie z art. 35 ust. 3 lit. c RODO, jest ona obowiązkowa dla monitorowania miejsc dostępnych publicznie. W jej przeprowadzeniu może być pomocny inspektor ochrony danych, jeżeli został wyznaczony.

Zgodnie z art. 35 ust. 7, ocena zawiera co najmniej:

a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie - prawnie uzasadnionych interesów realizowanych przez administratora;
b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1; oraz
d) 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.

**Zasady ograniczenia celu i minimalizacji wymagają ograniczenia obszaru monitorowania do niezbędnego zasięgu**. Należy mieć na uwadze, że interesy administratora nie mogą w każdej sytuacji w sposób nadmierny ograniczać prawa do prywatności i ochrony danych oraz uzasadnionego oczekiwania

osób obserwowanych co do zapewnienia intymności. Dlatego administrator powinien powstrzymywać się od prowadzenia monitoringu w obszarach wrażliwych, takich jak przebieralnie, toalety itp. Analogicznie prowadzenie monitoringu obejmującego obszar sąsiednich posesji może zostać uznane za nieproporcjonalne.

Istotne znaczenie ma **realizacja wobec osoby obserwowanej obowiązku informacyjnego ujętego w art. 13 RODO**. Musi on być, zgodnie z art. 12 rozporządzenia, realizowany w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część z wymienianych powyżej przepisów szczególnych wskazuje dodatkowo znaki lub ogłoszenia dźwiękowe, którymi należy oznaczyć pomieszczenia i teren monitorowany (w/w przepisy Kodeksu pracy i Prawa oświatowego). Pełna informacja o monitoringu, obejmująca wszystkie wymogi art. 13 RODO, powinna być dostępna w miejscu monitorowanym, np. na tablicach albo w formie dokumentu dostępnego na recepcji czy też u przedstawiciela administratora. Czyli możliwa jest realizacja obowiązku informacyjnego poprzez podanie informacji podstawowych i uzupełnienie ich w kolejnych warstwach informacyjnych. Znaki informujące o stosowaniu monitoringu mogą być dostępne przed wejściem w obszar obserwowany.

W art. 37 rozporządzenia wskazano, kiedy administrator wyznacza **inspektora ochrony danych (IOD)**. Z tą chwilą na inspektorze spoczywa m.in. prawny obowiązek monitorowania przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, a także realizacja działań zwiększających świadomość, szkolenie personelu uczestniczącego w operacjach przetwarzania oraz prowadzenie powiązanych z tym audytów oraz udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania (art. 39 ust. 1 lit. b i c RODO).

### 4.3. Podmiot przetwarzający

Zgodnie z art. 4 pkt 8 RODO, podmiotem przetwarzającym może być osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

Szczegółowe uregulowanie tego stosunku zawiera art. 28 rozporządzenia. Administrator może powierzyć wykonanie takiej usługi podmiotom, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą. Przetwarzanie przez podmiot przetwarzający odbywa się przede wszystkim na podstawie umowy, określającej:

a) przedmiot i czas trwania przetwarzania,

b) charakter i cel przetwarzania,

c) rodzaj danych osobowych oraz kategorie osób, których dane dotyczą,

d) obowiązki i prawa administratora.

Ponadto podmiot, któremu administrator danych powierzył ich przetwarzanie, odpowiada wobec administratora danych za przetwarzanie danych niezgodnie z zawartą umową. Zawarcie takiej umowy nie zmienia statusu ich administratora – jest w całości odpowiedzialny za ich prawidłowe przetwarzanie.

**W przypadku monitoringu wizyjnego może to dotyczyć zlecenia prowadzenia monitoringu w związku z ochroną obiektu przez profesjonalny podmiot.**

## 4.4. Odbiorca danych

W art. 4 pkt 9 RODO uregulowano definicję odbiorcy, która oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są uznawane za odbiorców, a przetwarzanie przez nie pozyskanych danych musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania. O odbiorcach albo ich kategoriach informować musi administrator. W praktyce oznaczać to może konieczność informowania osób obserwowanych w ramach realizacji obowiązku informacyjnego z art. 13 RODO, że dane mogą być przekazywane firmie chroniącej obiekt, która zarządza systemem, czy też osobom, które wykażą potrzebę uzyskania dostępu do nagrań (interes realizowany przez stronę trzecią), np. osobom poszkodowanym w sytuacjach zarejestrowanych przez kamery systemu. Nie jest wykluczone, że nagrania takie będą obejmować dane osobowe osób obserwowanych, które brały udział w zdarzeniu, a udostępnienie ich danych ma nadrzędny charakter wobec interesów lub podstawowych praw i wolności. Odbiorca danych ma obowiązek przetwarzać je zgodnie z zasadami ochrony danych i tylko w zakresie realizowanego przez siebie celu. Przykładowo, w razie nagrania uszkodzenia mienia przez drugą osobę (np. stłuczka na parkingu), zarządca terenu może podjąć decyzję o udostępnieniu nagrania obejmującego wizerunek sprawcy czy tablice rejestracyjne pojazdu osobie poszkodowanej, która chce dochodzić swoich praw. Musi to jednak odbywać się z poszanowaniem praw i wolności osób postronnych. Oznacza to, że nagranie nie powinno obejmować danych innych osób niezaangażowanych w zdarzenie.

W przypadku wniosków o dostęp do nagrań kierowanych do administratora przez organy publiczne i służby porządkowe, powinny być one związane z realizacją zadań tych podmiotów i zgodne z obowiązującymi je zasadami pozyskiwania danych osobowych.

W obu powyższych sytuacjach przypadki udostępnienia powinny być prawidłowo udokumentowane. W myśl zasady rozliczalności, jest to konieczne, by administrator mógł wykazać, że przetwarzał dane zgodnie z obowiązującym prawem.

# 5. Zabezpieczenie danych osobowych

Administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa uwzględniający stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania, a także ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze. Obejmuje to wymogi ujęte w sekcji II rozdziału 4 RODO – Bezpieczeństwo danych osobowych.

Administrator prowadzi dokumentację opisującą sposób przetwarzania danych oraz zastosowane środki techniczne i organizacyjne, a także ewidencję osób upoważnionych do ich przetwarzania. Do przetwarzania danych, o ile tak zdecyduje ich administrator, mogą być dopuszczone wyłącznie osoby działające z upoważnienia administratora lub podmiotu przetwarzającego i przetwarzają je wyłącznie na polecenie administratora.

W sytuacji, gdy przepisy szczególne nie określają wymogów co do środków technicznych i organizacyjnych, to administrator ma swobodę w tej materii i odpowiada za wykazanie, że są one wystarczające.

# 6. Opinie organów ochrony danych i dokumenty organów kontroli państwowej dot. monitoringu wizyjnego

## 6.1. Generalny Inspektor Ochrony Danych Osobowych

**6.1.1.** Wytyczne GIODO dotyczące wykorzystania monitoringu wizyjnego w szkołach

**6.1.2.** **Lekcje z GIODO -** Wykład 1. **Monitoring wizyjny w szkole** (VII edycja Programu "Twoje dane - Twoja sprawa")

## 6.2. Grupa Robocza art. 29

**6.2.1.** Dokument roboczy w sprawie przetwarzania danych osobowych przy nadzorze z użyciem kamer video (WP 67) – dostępny w wersji angielskiej

**6.2.2.** Opinia 4/2004 w sprawie przetwarzania danych osobowych przy nadzorze z użyciem kamer video (WP 89)

## 6.3. Europejski Inspektor Ochrony Danych

**6.3.1.** Wytyczne dot. monitoringu wizyjnego dla instytucji i agend Unii Europejskiej – dostępne w wersji angielskiej

## 6.4. Naczelna Izba Kontroli – informacje o wynikach kontroli

**6.4.1.** Funkcjonowanie miejskiego monitoringu wizyjnego i jego wpływ na poprawę bezpieczeństwa publicznego (nr P/13/154)

**6.4.2.** Wykorzystanie monitoringu wizyjnego w szkołach i jego wpływ na bezpieczeństwo uczniów (nr P/16/076)

**6.4.3.** Ochrona intymności i godności pacjentów w szpitalach (nr P/17/103)

# III. Lista pytań dotycząca praktycznych zagadnień związanych z przetwarzaniem danych osobowych

## 1. Co powinno się wziąć pod uwagę przed podjęciem decyzji w sprawie instalacji monitoringu w szkole?

Monitoring wizyjny jest narzędziem ingerencji w konstytucyjnie chronione prawo jednostki do prywatności. Dlatego wszelkie działania ingerujące w to prawo powinny być dokonywane rozważnie i z poszanowaniem obowiązujących przepisów prawa - zgodnie z **zasadą legalizmu** wyrażoną w art. 7 Konstytucji RP. W szczególności dotyczy to ochrony prawa do prywatności dziecka.

Ponadto administrator powinien zadać sobie pytanie o **adekwatność wprowadzenia monitoringu wizyjnego**, **jako metody zapewnienia bezpieczeństwa czy ochrony mienia.** Dyrektor szkoły powinien ocenić, czy inne, mniej ingerujące w prywatność rozwiązania nie przyniosłyby oczekiwanych i wystarczających efektów w zakresie zapewnienia bezpieczeństwa. Elementem dokonywanej oceny powinna być zatem analiza potrzeb i celowości budowy systemu wideomonitoringu wraz z prognozą jego skuteczności w kontekście wpływu na prywatność (*privacy impact assessment)*. Może się bowiem okazać, że rozwiązania mniej inwazyjne stanowią alternatywę dla kosztownego systemu monitoringu i z powodzeniem mogą go zastąpić.

Monitoring wizyjny stwarza również ryzyko **przetwarzania danych osobowych innych osób (niebędących pracownikami czy też użytkownikami, jak uczniowie szkół),** które mogą znaleźć się w obszarze monitorowanym (wejścia na teren, jego otoczenie – ulice, chodniki, boiska czy place zabaw). Wobec tych osób administrator ma obowiązek poinformowania o stosowaniu obserwacji, zapewnienia dostępu do ich danych i ich zabezpieczenia. Pamiętać też należy, że przy okazji system monitoringu mógłby zostać również pośrednio wykorzystany jako **narzędzie nadzoru i kontroli pracy.** Kwestia ta została omówiona poniżej, w odpowiedzi na pytanie 4.

## 2. Jaka jest podstawa prawna instalowania monitoringu?

Rozważając zagadnienie podstawy prawnej przetwarzania danych osobowych przez ich administratora za pomocą systemu monitoringu wskazać należy, że odrębne przepisy prawa regulują niektóre przypadki ochrony osób i mienia przez określone podmioty za pomocą monitoringu wizyjnego, np. wspomniane już przepisy Kodeksu pracy, Prawa oświatowego, czy przepisy ustaw o samorządach: gminnym, powiatowym, i województwa, a także przepisy ustawy o zasadach zarządzania mieniem państwowym.

W przypadkach nieuregulowanych przez przepisy szczególne, jako podstawę prawną przetwarzania danych osobowych w zakresie wizerunku przez podmioty sektora prywatnego należy wskazać **przesłankę legalności określoną w art. 6 ust. 1 lit. f rozporządzenia 2016/679**, uznając

zapewnienie bezpieczeństwa osób i mienia w obszarze objętym monitoringiem za prawnie usprawiedliwiony cel administratora danych.

Podkreślenia wymaga, że zgodnie ze stanowiskiem Trybunału Sprawiedliwości UE wyrażonym w wyroku w sprawie C-212/13 Ryneš[5], ochrona osób i mienia może być uznana za uzasadniony interes administratora w rozumieniu art. 7 lit. f) dyrektywy 95/46/WE. **Każdorazowo musi to się jednak wiązać z poszanowaniem praw i wolności osoby obserwowanej oraz wypełnianiem obowiązków ustawowych administratora.** Oznacza to m.in. poszanowanie prywatności osób w obszarach podwyższonego oczekiwania prywatności (przebieralnie itp.) oraz realizowania obowiązków informacyjnych wobec osób obserwowanych.

Należy pamiętać, że art. 6 ust. 1 lit f RODO w odniesieniu do podmiotów z sektora publicznego art. 6 ust. 1 lit f RODO nie będzie mieć zastosowania.

### 3. Czy administrator może zainstalować atrapy kamer monitoringu?

Stanowisko organu ds. ochrony danych osobowych jest w tej kwestii niezmienne – **stosowanie atrap powinno być zakazane**. Atrapy kamer z jednej strony wprowadzają u potencjalnie monitorowanych poczucie ingerencji w sferę prywatności, a z drugiej mylne poczucie zwiększonego bezpieczeństwa. Niepożądane skutki związane z wykorzystaniem monitoringu, także z atrapami kamer, czy to w otwartej przestrzeni, jak np. boiska szkolne, czy też w zamkniętej, jak np. szatnie czy korytarze, mogą przeważać nad ewentualnymi korzyściami wynikającymi z ich stosowania i tym samym podawać w wątpliwość skuteczność i adekwatność tego narzędzia w realizacji zamierzonego celu w danych okolicznościach.

### 4. Czy monitoring w miejscu pracy może zostać wykorzystany do kontroli pracy?

Możliwość stosowania określonych narzędzi kontroli pracownika co do zasady powinna być określona w ustawie, wraz z gwarancjami zabezpieczającymi pracowników przed ich nadużywaniem ze strony administratora. W myśl przepisów Kodeksu pracy, monitoring ma służyć zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. W tych celach nie mieści się stosowanie monitoringu jako środka nadzoru nad jakością wykonywania pracy. Choć mogą istnieć pokusy, by monitoring przy okazji był narzędziem np. kontroli długości przerw czy opuszczania przez pracownika miejsca pracy, a także obserwacji czynności wykonywanych podczas świadczenia pracy. Wyraźnie to podkreśla art. 180a ust 2 Prawa oświatowego. Dlatego niedopuszczalne jest instalowanie monitoringu w klasach, w których

[5] Wyrok Trybunału Sprawiedliwości z dnia 11 grudnia 2014 r. w sprawie C-212/13 František Ryneš przeciwko Úřad pro ochranu osobních údajů

podczas trwania zajęć lekcyjnych to nauczyciel (nie zaś kamera monitoringu wizyjnego) sprawuje nadzór nad bezpieczeństwem uczniów i mienia. To samo dotyczy nadzorowania pracowników przez ich przełożonego. Zgodnie z Konstytucją RP, RODO czy Kodeksem pracy, podmioty stosujące monitoring powinny kierować się przede wszystkim zasadami celowości i minimalizacji danych. Przewidują one, że dane muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach. Ponadto, pozyskiwać można jedynie te dane, które są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Innymi słowy, wymagane jest stosowanie tylko środków proporcjonalnych do celów przetwarzania danych osobowych. W przypadku monitoringu celem tym jest **zapewnienie bezpieczeństwa i ochrony osób oraz mienia,** nie zaś nadzór nad efektywnością czy wydajnością wykonywanej przez pracownika pracy.

## 5. Jakie obowiązki wobec osób obserwowanych ma administrator stosujący monitoring wizyjny?

Administrator powinien na swoim terenie poinformować osoby, które potencjalnie mogą zostać nim objęte, że monitoring jest stosowany i jaki obszar jest nim objęty. Podać swoją nazwę, adres, obszar oraz cel monitorowania i inne informacje ujęte w art. 13 RODO.

Osoby pozostające w obszarze monitorowanym muszą mieć świadomość, że w miejscu, w którym się znajdują, prowadzone są czynności monitoringu. Tablice informujące o zainstalowanym monitoringu powinny być widoczne, syntetyczne, umieszczone w sposób trwały w niezbyt dużej odległości od nadzorowanych miejsc, zaś wymiary tablic muszą być proporcjonalne do miejsca, gdzie zostały umieszczone. Stosowane mogą być dodatkowo piktogramy informujące o objęciu dozorem kamer.

Nie jest wystarczające oznaczenie obszaru objętego monitoringiem jedynie piktogramami, gdyż należy również spełnić obowiązek informacyjny określony w art. 13 RODO. Nie oznacza to jednak konieczności umieszczania wszystkich informacji wskazanych w tym przepisie. W takiej sytuacji możliwe zastosowanie warstwowych not informacyjnych.

Administrator powinien niezwłocznie odpowiadać na wszelkie pytania osoby obserwowanej w ramach przysługujących jej uprawnień, przede wszystkim zgodnie z art. 12 – 22 RODO.

## 6. Jakie prawa przysługują osobom objętym monitoringiem?

Każdej osobie przysługuje prawo do informacji o objęciu jej monitoringiem wizyjnym oraz prawo do ochrony swojego wizerunku przed rozpowszechnianiem, chyba że przepisy odrębne stanowią inaczej. Obowiązek udzielenia takich informacji wynika z art. 13 RODO, zaś przepisy rozdziału III szczegółowo określają prawa osoby, której dane dotyczą.

Prawa osób objętych monitoringiem obejmują m.in.:

- **prawo do informacji** o istnieniu monitoringu w określonym miejscu, jego zasięgu, celu, nazwie podmiotu odpowiedzialnego za instalację, jego adresie i danych do kontaktu;
- **prawo dostępu do nagrań** w uzasadnionych przypadkach;
- **prawo żądania usunięcia danych jej dotyczących;**
- **prawo do anonimizacji wizerunku** na zarejestrowanych obrazach i/lub usunięcia dotyczących jej danych osobowych;
- **prawo do przetwarzania danych przez ograniczony czas.**

### 7. Jakie warunki powinny być spełnione w związku z instalacją kamer w szkole?

Szkoła, jako podmiot odpowiedzialny za instalację monitoringu, a następnie za gromadzenie i przechowywanie zapisów z kamer, musi stosować się wprost do przepisów Prawa oświatowego i rozporządzenia 2016/679. Podstawowym warunkiem stosowania monitoringu wizyjnego w szkole jest uprzednie poinformowanie całej społeczności szkolnej o instalacji tego systemu poprzez wywieszenie w widocznych miejscach tablic informacyjnych na ten temat. Powinny one informować nie tylko o obecności kamer monitoringu wizyjnego i jego zasięgu, ale m.in. również o celu ich instalacji i warunkach, na jakich szkoła stosuje to narzędzie nadzoru. Ważne jest również poinformowanie o przysługującym osobie monitorowanej prawie do kontroli dotyczących jej danych osobowych.

Podkreślenia wymaga, że zgodnie z art. 39 ust. 1 pkt 5a ustawy o systemie oświaty, to **dyrektor szkoły** wykonuje zadania związane z zapewnieniem bezpieczeństwa uczniom i nauczycielom w czasie zajęć organizowanych przez szkołę, a zgodnie z ust. 4 przywołanego przepisu, przy wykonywaniu swoich zadań współpracuje z radą pedagogiczną, rodzicami i samorządem uczniowskim. **Zasada ta została zachowana w art. 108a Prawa oświatowego, zgodnie z którym cała społeczność szkolna powinna współpracować z dyrektorem i organem prowadzącym w kwestii podjęcia decyzji o uruchomieniu monitoringu wizyjnego na terenie placówki. Niezależnie od powyższego dyrektor powinien przeprowadzić ocenę ryzyka.** Pamiętać przy tym także należy, że wprowadzenie monitoringu powinno być poprzedzone analizą w zakresie możliwości zastosowania innych, mniej ingerujących w prywatność środków. **Tam, gdzie monitoring już istnieje, powinny być natomiast przeprowadzane konsultacje wraz z przeglądem stanu bezpieczeństwa w związku ze stosowaniem monitoringu, także w celu podjęcia decyzji, czy jego stosowanie jest nadal zasadne.** Wpływ systemu monitoringu na bezpieczeństwo powinien być okresowo badany, celem stwierdzenia, czy rozwiązanie takie przynosi zamierzone skutki i nie narusza w sposób nadmierny praw osób obserwowanych.

### 8. Co oznacza zasada ograniczenia celu?

Administrator, który zamierza wprowadzić monitoring, powinien wykazać zasadność jego stosowania, w tym **proporcjonalność tego środka do celu**, jakiemu ma służyć (np. poprawa bezpieczeństwa). Zasada ta dotyczy przede wszystkim decyzji, czy monitoring w istocie musi być stosowany i jakie argumenty przeważają, by uznać, że jest on lepszym środkiem niż inne dostępne służące bezpieczeństwu bądź jego poprawie oraz czy niepożądane negatywne skutki nie przeważają nad taką formą kontroli. Systemy monitoringu powinny być stosowane po uprzednim rozważeniu, czy inne środki prewencyjne czy ochrony, niewymagające pozyskiwania obrazu, nie okażą się ewidentnie niewystarczające lub niemożliwe do zastosowania Na przykład, gdy brak jest wystarczającej liczby nauczycieli i pracowników do pełnienia dyżuru, albo jest zbyt duży obszar, aby można było objąć wszystkie newralgiczne miejsca taką formą nadzoru.

Następnie, o ile zdecydowano o wyborze monitoringu jako rozwiązania niezbędnego, dojść powinno do wyboru odpowiedniej technologii, kryteriów wykorzystywania urządzeń w konkretnych sytuacjach oraz ustaleń dotyczących przetwarzania danych, odnoszących się także do zasad dostępu i okresu przechowywania. Zasada ta oznacza także, że urządzenia służące do takiego nadzoru mogą być stosowane wyłącznie jako środki pomocnicze, gdy cel rzeczywiście uzasadnia ich użycie.

Administrator musi też ustalić, które przepisy szczególne będą miały zastosowanie do wdrażanego przez niego systemu monitoringu, gdy różnie określają one dopuszczalne cele monitoringu. Dla przykładu:

- pracodawca może stosować monitoring, gdy 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;
- dyrektor szkoły może wprowadzić monitoring, gdy jest to niezbędne do zapewnienia bezpieczeństwa uczniów i pracowników lub ochrony mienia;
- gmina lub powiat mogą stosować monitoring w celu zapewnienia porządku publicznego i bezpieczeństwa obywateli oraz ochrony przeciwpożarowej i przeciwpowodziowej.

## 9. W jakich miejscach monitoring może być instalowany?

Administrator, po przeanalizowaniu czy korzyści z instalacji monitoringu przeważają nad jego niepożądanymi skutkami, decydując o montażu systemu monitoringu, powinien pamiętać o istnieniu tych przestrzeni, w których monitoring jest niedopuszczalny. Chodzi głównie o takie miejsca, jak przebieralnie, szatnie, toalety, natryski czy łazienki.

Kodeks pracy wprost wskazuje, że monitoring nie obejmuje pomieszczeń sanitarnych, szatni, stołówek oraz palarni lub pomieszczeń udostępnionych zakładowej organizacji związkowej. Natomiast Prawo oświatowe do obszarów zakazanych zalicza pomieszczenia, w których odbywają się zajęcia dydaktyczne, wychowawcze i opiekuńcze, czy te pomieszczenia, w których uczniom jest udzielana pomoc psychologiczno – pedagogiczna, jak również pomieszczenia przeznaczone do odpoczynku i rekreacji pracowników, sanitarnohigieniczne, gabinet profilaktyki zdrowotnej, a także szatnie i przebieralnie. **Miejsca monitorowane powinny być**

**wyznaczone tam, gdzie dochodzi do incydentów albo istnieje realne zagrożenie dla bezpieczeństwa, zaś niemożliwe jest objęcie takich miejsc innymi formami nadzoru, jak np. w przypadku szkół dyżurami nauczycieli czy pracowników.**

Natomiast w odniesieniu do innych miejsc instalowania kamer należy rozważyć, czy ich usytuowanie nie narusza w szczególności zasady proporcjonalności. Np. kamery nie powinny być bezpośrednio skierowane na ekran komputera pracownika i umożliwiać śledzenia wykonywanych przez niego czynności na tym urządzeniu, ponieważ monitoring nie powinien być wykorzystywany do nadzorowania wykonywania obowiązków służbowych. Pamiętać także należy, że niektóre strefy w miejscu pracy, takie jak biurko czy szafka, objęte są szczególnie silnym i uzasadnionym oczekiwaniem prywatności.

### 10. Jaki jest okres przechowywania nagrań z monitoringu?

Okres retencji danych, czyli ich przechowywania po dokonaniu nagrania, nie jest w polskich przepisach jednoznacznie określony. Przykładowo w przepisach Kodeksu pracy, Prawa oświatowego i ustawy o samorządzie gminnym wskazano **maksymalny 3-miesięczny okres**. Jednak biorąc pod uwagę, że celem wdrażania monitoringu jest przeciwdziałanie szkodom na osobach i mieniu, **należy w miarę możliwości przyjmować krótszy czas przechowywania**. Powoduje to nie tylko mniejszą ingerencję w prywatność osób obserwowanych, ale także zmniejszenie kosztów utrzymania systemu. Ponadto należy wziąć pod uwagę, że np. szkoły i zakłady pracy są obiektami stale dozorowanymi przez pracowników – nauczycieli pełniących dyżury, ochronę i stróżów. Obraz z kamer może być na bieżąco obserwowany przez operatora lub przechowywany w celu udokumentowania incydentów, jednak nie dłużej niż jest to konieczne do zakończenia odpowiednich czynności wyjaśniających. Przede wszystkim należy pamiętać o przepisie art. 5 ust. 1 lit. e RODO, w którym wskazano, że **dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane**. Okres ten powinien być raczej liczony w tygodniach niż w miesiącach. Należy jednocześnie pamiętać, że nagrania dotyczące incydentów mogą być przechowywane dłużej – do czasu wyjaśnienia sprawy albo zakończenia odpowiednich postępowań.

### 11. Czy przepisy o ochronie danych osobowych zawsze mają zastosowanie do monitoringu?

Nie zawsze monitoring wizyjny wiąże się z przetwarzaniem danych osobowych. Rozporządzenie 2016/679 i krajowe przepisy szczególne można zastosować do monitoringu, jeśli jest on wykorzystywany w celu przetwarzania danych osobowych. Jeżeli monitoring służy jedynie do podglądu danego miejsca, a nagranie nie jest zachowywane na twardym dysku komputera czy innym nośniku, to wówczas trudno mówić o przetwarzaniu danych osobowych. Z danymi osobowymi mamy do czynienia wówczas, gdy obraz z kamer zawiera wizerunki osób i jest utrwalony w systemie monitoringu na nośnikach danych. Pamiętać przy tym

należy, że podmioty wykorzystujące systemy monitoringu z reguły utożsamiają przetwarzanie danych z działaniem podejmowanym w celu identyfikacji konkretnych osób na podstawie nagrań. Tymczasem w rozporządzeniu za przetwarzanie danych uznaje się już ich gromadzenie.

### 12. Kto jest osobą odpowiedzialną za przetwarzanie danych osobowych pozyskanych w związku z zastosowaniem monitoringu?

Administrator jest odpowiedzialny za zapewnienie bezpieczeństwa funkcjonowania systemu monitoringu wizyjnego i przetwarzanie danych osobowych pozyskanych tą drogą. Zgodnie z art. 4 pkt 7 rozporządzenia, 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. O tym, kto jest administratorem danych, decydują również przepisy szczególne. Dla przykładu z taką sytuacją mamy do czynienia w przypadku szkoły. Kierujący i reprezentujący ją **dyrektor ma zapewnić, aby przetwarzanie danych osobowych uczniów i ich rodziców lub opiekunów prawnych, nauczycieli i innych pracowników szkoły lub osób znajdujących się na terenie tej placówki** odbywało się zgodnie z prawem. Ponadto jest on odpowiedzialny za działania wszystkich osób upoważnionych do przetwarzania danych, w tym inspektora ochrony danych – jeśli został przez niego powołany.

**Zgodnie z art. 108a Prawa oświatowego, dyrektor podejmuje decyzję w uzgodnieniu z organem prowadzącym szkołę lub placówkę po przeprowadzeniu konsultacji z radą pedagogiczną, radą rodziców i samorządem uczniowskim. Nie oznacza to, że mamy do czynienia z instytucją współadministrowania, o której mowa w art. 26 RODO.**

Fakt, że zapisy z monitoringu nie zawsze są związane z przetwarzaniem danych osobowych, wcale nie zwalnia szkoły, która jest w ich posiadaniu, z obowiązku zabezpieczenia takich informacji przed dostępem do nich osób nieuprawnionych. Jeśli takie nagranie zostałoby wykorzystane do innych celów (np. opublikowane w Internecie), wówczas podmiot danych może dochodzić swych praw przed sądem.

Pamiętać także należy, że niejednokrotnie dochodzi do udostępnienia danych osobowych innym podmiotom na zasadzie zlecenia organizacji czy wykonania jakiejś czynności, np. przy prowadzeniu obsługi całego systemu monitoringu. Zgodnie z art. 28 RODO, jest to dopuszczalne tylko na podstawie **umowy zawartej na piśmie**. Podmiot, któremu zlecono takie operacje, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie oraz jest zobowiązany do odpowiedniego zabezpieczenia danych zgodnie z przepisami o ochronie danych osobowych.

### 13. Jakie działania powinien podjąć administrator w kwestii zabezpieczenia danych osobowych pozyskanych z monitoringu?

Niezależnie od wymogów zabezpieczenia danych określonych w przepisach szczególnych, zgodnie z rozdziałem IV RODO (art. 24 i n.), administrator, uwzględniając charakter, zakres, kontekst i cele

przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane. W szczególności powinno się zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Ponadto osoby, które zostaną upoważnione do dostępu do systemów monitoringu, mają obowiązek zachowania w poufności informacji uzyskanych w trakcie prowadzenia monitoringu oraz tych, dotyczących bezpieczeństwa funkcjonowania tych systemów. Ważne jest, aby osoba upoważniona do przetwarzania danych, nie mogła wykorzystywać ich na swoją rzecz i w innych celach, np. opublikowania w Internecie. Wówczas podmiot danych może dochodzić swych praw przed organem nadzorczym albo sądem cywilnym.

### 14. Czy szkoła bez monitoringu może być bezpiecznym miejscem nauki i pracy?

Każdorazowe wprowadzenie monitoringu powinno podlegać ocenie zgodnie z zasadą proporcjonalności ujętą w art. 31 ust. 3 Konstytucji RP. Natomiast prawo do ochrony informacji dotyczącej osoby ujęte w art. 51 Konstytucji RP, może być ograniczone m.in. gdy jest to konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku prawnego. Dlatego przy podejmowaniu decyzji o wprowadzeniu do szkoły monitoringu należy zachować równowagę pomiędzy zagwarantowaniem praw jednostki (uczniów, nauczycieli i innych pracowników szkoły, a także rodziców i osób odwiedzających placówkę) a ogólnym interesem szkoły. Decyzja, czy monitoring powinien być zainstalowany, powinna opierać się na ocenie efektywności innych, alternatywnych i możliwych do zastosowania środków mogących zapewnić bezpieczeństwo. Jak pokazuje praktyka, często zabezpieczenia te nie muszą być wygórowane, skomplikowane i zarazem kosztowne. Niejednokrotnie wystarczające jest zastosowanie innych niż monitoring wizyjny ogólnodostępnych środków technicznych, które mogą stanowić alternatywę dla kosztownego systemu monitoringu i z powodzeniem go zastąpić. To samo odnosi się do działań organizacyjnych, które w dużej mierze mogą odwoływać się do wyobraźni i być wyrazem zdrowego rozsądku. Zastosowanie systemu monitoringu w szkole powinno być zawsze przemyślane i ograniczone do obszarów, gdzie jest to niezbędne z punktu widzenia bezpieczeństwa oraz stosowane z uwzględnieniem wpływu na prywatność uczniów, nauczycieli i innych osób.

### 15. Czy monitoring może polegać na montowaniu ukrytych kamer?

Przepisy RODO oraz unormowania krajowe nie pozwalają, by monitoring był prowadzony przy pomocy ukrytych kamer. Uprawnienia do prowadzenia niejawnego monitorowania mają jedynie służby porządkowe i specjalne prowadzące czynności na podstawie ustaw regulujących ich działalność. Stosowanie ukrytych kamer może zostać uznane za nadmiarową formę przetwarzania danych, wiązać się z odpowiedzialnością

administracyjną i cywilną, a nawet karną. Obszary objęte monitoringiem wizyjnym muszą być oznaczone zgodnie z wymogami określonymi w przepisach szczególnych oraz RODO.

**16. Czy monitoring może polegać na montowaniu kamer umożliwiających rejestrację dźwięku?**

Przepisy o monitoringu nie zezwalają co do zasady na nagrywanie dźwięku towarzyszącego zdarzeniom. Takie uprawnienia posiadają jedynie służby porządkowe i specjalne na podstawie ustaw regulujących ich działalność. Stosowanie rejestracji dźwięku może zostać uznane za nadmiarową formę przetwarzania danych, wiązać się z odpowiedzialnością administracyjną i cywilną, a nawet karną.

**17. Czy przepisy o monitoringu wprowadzone w ustawie o ochronie danych osobowych mają zastosowanie do istniejących już systemów?**

Przepisy RODO oraz ustaw szczególnych mają zastosowanie do wszystkich objętych nimi systemów monitorowania przestrzeni. Oznacza to, że istniejące systemy muszą zostać pilnie dostosowane do nowych wymogów. Oczywiście organ nadzorczy zdaje sobie sprawę, że przystosowanie systemów do nowych przepisów wymaga przeprowadzenia konsultacji z zaangażowanymi podmiotami, zmian dokumentów wewnętrznych oraz spełnienia obowiązków wobec osób obserwowanych. **Dlatego w pierwszej kolejności monitorowane będą postępy administratorów w dostosowaniu do nowych wymogów. Działania takie powinny być przez administratorów i podmioty przetwarzające podejmowane niezwłocznie, tak by wykazać dążenie do zapewnienia zgodności z obowiązującym prawem. W dalszej kolejności prowadzone będą przez Prezesa Urzędu Ochrony Danych Osobowych działania weryfikujące wypełnianie zasad stosowania monitoringu wizyjnego przewidzianych w RODO oraz przepisach szczególnych.**

**18. W jaki sposób szkoła lub zakład pracy – które monitorują np. szatnie – mają zastosować środki techniczne uniemożliwiające rozpoznanie osób przebywających w tym pomieszczeniu?**

Środki techniczne uniemożliwiające rozpoznanie osób zostały wskazane w art. $22^2$ § 2 Kodeksu pracy oraz art. 108a ust. 3 Prawa oświatowego jako przykładowe rozwiązania zapewniające ochronę godności oraz innych dóbr osobistych osób obserwowanych. Możliwe jest stosowanie oprogramowania zamazującego określone fragmenty kadrowanego obrazu (w tym postacie osób obserwowanych), czy też takie ustawienie kamer, by naruszenie godności oraz innych dóbr osobistych, czy też zasady wolności i niezależności związków zawodowych, było niemożliwe. Rozwiązania techniczne mające na celu zminimalizowanie ryzyka naruszenia praw lub wolności osób, których dane dotyczą, w odniesieniu do monitoringu miejsc, w których co do zasady taki monitoring jest zakazany powinny uwzględniać **zasadę zapewnienia ochrony danych osobowych na etapie projektowania i domyślnej ochrony danych ujęte w art. 25 RODO**. Należy pamiętać, że pomieszczenia wyłączone z monitoringu mogą być nim objęte tylko wyjątkowo, ze względu na istniejące zagrożenie dla realizacji celu (bezpieczeństwo osób i mienia itd.). Może to np. oznaczać tymczasowe objęcie nadzorem

kamer szafek, do których ktoś usiłował się włamać albo dokonał z nich kradzieży. Nie stanowi to podstawy do nieograniczonego w czasie monitorowania tych obszarów. W każdej sytuacji administrator powinien bardzo ostrożnie podchodzić do monitorowania miejsc zakazanych i zapewnić proporcjonalność takich działań, gdyż może to się wiązać ze skargami osób obserwowanych oraz odpowiedzialnością administracyjną i cywilną.

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