GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH
dr Edyta Bielak-Jomaa

Warszawa, dnia 26 stycznia 2017 r.

DES(WOM-070-9/17/8493

Pani
Anna Zalewska
Minister Edukacji Narodowej
Al. J. Ch. Szucha 25
00-918 Warszawa

Szanowna Pani Minister,

w ślad za wcześniejszymi ustaleniami, mam przyjemność złożyć na ręce Pani Minister dokument pt. „Wytyczne Generalnego Inspektora Ochrony Danych Osobowych dotyczące wykorzystania monitoringu wizyjnego w szkołach", będący odpowiedzią organu ds. ochrony danych osobowych na opracowany przez Ministerstwo Edukacji Narodowej rządowy program wspomagania w latach 2015 – 2018 organów prowadzących szkoły w celu zapewnienia bezpiecznych warunków nauki, wychowania i opieki w szkołach – „Bezpieczna+" w 2016 r.

Z wyrazami szacunku

RPW/6338/2017 P
Data:2017-02-06

2017 -02- 06
Podpis .....

ul. Stawki 2, 00-193 Warszawa
tel. 22 531-03-88
fax 22 531-03-99
www.giodo.gov.pl

Wytyczne Generalnego Inspektora Ochrony Danych Osobowych dotyczące wykorzystywania monitoringu wizyjnego w szkołach

I. Informacje ogólne

Niniejszy dokument został przygotowany na podstawie art. 12 pkt. 6 ustawy o ochronie danych osobowych jako materiał edukacyjny. Wiążąca ocena prawidłowości operacji przetwarzania danych osobowych, jaką jest stosowanie **monitoringu wizyjnego**, jest każdorazowo prowadzona przez Generalnego Inspektora Ochrony Danych Osobowych w trybie właściwych postępowań, o których mowa w art. 12 pkt 1 i 2 ustawy, tj. w toku kontroli zgodności przetwarzania z przepisami albo ze skargi na przetwarzanie danych osobowych.

1. Obowiązujące przepisy

Funkcjonowanie szkół i innych placówek oświatowych nie jest możliwe bez przetwarzania danych osobowych wszystkich związanych z nimi osób – uczniów, rodziców, opiekunów prawnych, nauczycieli i innych pracowników, a nawet odwiedzających gości.

Proces ten podlega rygorom określonym przepisami **ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych** (t.j. Dz. U. z 2016 r. poz. 922), zwanej dalej ustawą i aktów wykonawczych do niej.

Wśród nich wymienić należy:

a) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych wraz załącznikiem zawierającym opis środków bezpieczeństwa na poziomie podstawowym, podwyższonym i wysokim (Dz. U. Nr 100, poz. 1024);

b) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. Nr 229, poz. 1536);

c) rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. z 2014, poz. 1934);

d) rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. z 2015, poz. 719);

e) rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. z 2015, poz. 745).

2. Definicja danych osobowych

Każdy ma prawo do ochrony dotyczących go danych osobowych. Ustawa wprowadza normy służące realizacji tego prawa. W szczególności reguluje postępowanie przy przetwarzaniu danych osobowych, czyli wszelkich operacjach na nich wykonywanych, takich, jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie. Przetwarzanie danych osobowych może mieć miejsce ze względu na dobro publiczne, dobro osoby, której dane dotyczą, lub dobro osób trzecich w zakresie i trybie określonym ustawą. Ustawę stosuje się do przetwarzania danych osobowych w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych, jak również w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych.

Za **dane osobowe** uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, pozwalające na określenie tożsamości tej osoby. 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.

Możliwa do zidentyfikowania jest więc taka osoba, której tożsamość można określić bezpośrednio lub pośrednio, zwłaszcza poprzez powołanie się na numer identyfikacyjny, albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

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

a) dane tzw. zwykłe, takie jak np. imię, nazwisko, adres zamieszkania, data i miejsce urodzenia, numer telefonu, wykonywany zawód, itp.

b) dane szczególnie chronione (tzw. dane wrażliwe, sensytywne), wymienione w art. 27 ust. 1 ustawy:

- dane ujawniające pochodzenie rasowe lub etniczne,
- poglądy polityczne,
- przekonania religijne lub filozoficzne,
- przynależność wyznaniowa, partyjna lub związkowa,
- dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym,
- dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych,
- inne orzeczenia wydane w postępowaniu sądowym lub administracyjnym.

Przetwarzanie danych wrażliwych wiąże się z koniecznością wypełnienia dodatkowych gwarancji ich ochrony (art. 27 ust. 2 ustawy).

3. Zbiór danych

Zbiorem danych, w rozumieniu art. 7 pkt 1 ustawy, jest każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie. Zbiorem danych jest zestaw informacji charakteryzujący się następującymi cechami:

a) jest to zestaw danych osobowych, tj. informacji o charakterze osobowym;

b) posiada ustaloną strukturę, co oznacza, że dane są uporządkowane i ułożone w odpowiedni sposób;

c) dane w nim zawarte są dostępne według określonych kryteriów, co oznacza, że istnieje pewien klucz ich wyszukiwania w zbiorze, pozwalający na w miarę szybkie i bezpośrednie odszukanie interesujących danych osobowych, bez konieczności przeglądania całego zbioru lub znacznej jego części; nie ma przy tym znaczenia liczba ani rodzaje kryteriów - może to być zarówno kryterium osobowe (np. imię, nazwisko, data urodzenia, PESEL) lub nieosobowe (np. data zamieszczenia danych w zbiorze, liczba porządkowa).

Pojęcie zbioru danych obejmuje swym zakresem zarówno zbiory zautomatyzowane, przetwarzane przy użyciu aplikacji bazujących na systemach zarządzających bazami danych, jak i niezautomatyzowane (manualne, tradycyjne). Zbiorami danych mogą być więc np. ręcznie tworzone zbiory ewidencyjne, zgromadzone akta osobowe (teczki, kartoteki), a także formularze czy kwestionariusze, uporządkowane i ułożone w odpowiedni sposób.

Jednym ze szczególnych rodzajów zbiorów danych przetwarzanych przy użyciu systemów informatycznych są zbiory danych w postaci plików danych stanowiących nagranie obrazów zarejestrowanych przez kamery systemu monitoringu wizyjnego.

4. Przetwarzanie danych

Ustawa o ochronie danych osobowych określa zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób fizycznych, których dane są lub mogą być przetwarzane w zbiorach danych.

Przetwarzaniem danych są wszelkie czynności (zarówno statyczne, jak i dynamiczne) wykonywane na danych osobowych, jak np. zbieranie, utrwalanie, opracowywanie, zmienianie, udostępnianie, usuwanie, przechowywanie (archiwizowanie), czy też operacje wykonywane w systemach informatycznych, jak wysyłanie e-maila, sms-a, itp. **Przetwarzanie danych zwykłych może się odbywać jedynie po spełnieniu jednego z warunków określonych w art. 23 ust. 1 pkt 1-5 ustawy (dane tzw. zwykłe) i/lub w art. 27 ust. 2 pkt 1-10 ustawy (dane szczególnie chronione).**

Podstawą przetwarzania danych zwykłych może być :

- zgoda osoby, której dane dotyczą, chyba że chodzi o usunięcie jej danych,
- niezbędność realizowania uprawnienia lub obowiązku wynikającego z przepisu prawa,
- konieczność realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie tej osoby,
- określone prawem zadanie realizowane dla dobra publicznego, prawnie usprawiedliwiony cel realizowany przez administratorów danych (odbiorców danych), jeżeli przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Przetwarzanie danych szczególnie chronionych, co do zasady, jest zabronione z wyjątkiem sytuacji określonych w art. 27 ust. 2 ustawy, np. gdy osoba, której dane dotyczą wyrazi na to zgodę na piśmie (chyba że chodzi o usunięcie jej danych), przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez jej zgody i stwarza pełne gwarancje ich ochrony, przetwarzanie takich danych jest niezbędne do ochrony żywotnych interesów podmiotu danych lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do

wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora, albo przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem czy prowadzenia badań naukowych i in.

5. Podstawowe zasady ochrony danych osobowych

Główne zasady postępowania przy przetwarzaniu danych osobowych wyznacza art. 26 ust. 1 ustawy, ujmując je w formę podstawowych obowiązków administratora danych. Z jego treści wynika, że administrator danych powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a co za tym idzie, ma on przestrzegać wskazanych poniżej zasad:

1. legalności – dane mogą być przetwarzane tylko na podstawie przepisów prawa,
2. celowości – dane powinny być zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu, jeśli jest to niezgodne z tymi celami,
3. merytorycznej poprawności – dane powinny być merytorycznie poprawne,
4. adekwatności – dane powinny być adekwatne (niezbędne, proporcjonalne) w stosunku do celów, w jakich są przetwarzane,
5. ograniczenia czasowego – dane w postaci umożliwiającej identyfikację osób, których dotyczą, nie mogą być przetwarzane dłużej, niż jest to niezbędne do osiągnięcia celu, dla którego zostały zebrane.

Ustawa daje osobom możliwość skorzystania z prawa do formalnej kontroli przetwarzania dotyczących ich danych, które ustanowione jest w rozdziale 4 ustawy – Prawa osoby, której dane dotyczą. Mogą oni domagać się zwłaszcza: uzyskania informacji, czy zbiór danych istnieje, ustalenia administratora danych, adresu jego siedziby; uzyskania informacji o celu, zakresie i sposobie przetwarzania danych oraz informacji o źródle, z którego dane pochodzą; żądania uzupełnienia, uaktualnienia, sprostowania, a nawet czasowego lub stałego wstrzymania przetwarzania danych lub ich usunięcia, jeżeli są one nieaktualne, niekompletne, nieprawdziwe lub zostały zebrane z naruszeniem prawa albo są już zbędne do realizacji celu, dla którego były zebrane. Ustawa przyznaje osobom także prawo do sprzeciwu, gdy administrator przetwarza dane w celach innych niż te, dla których były zbierane lub przekazuje je innemu administratorowi danych. W takiej sytuacji przysługuje im prawo żądania od administratora danych odpowiedniego zachowania się w przypadku nieprzestrzegania ustawy, a także prawo występowania do Generalnego Inspektora Ochrony Danych Osobowych, organów ścigania oraz wymiaru sprawiedliwości w sprawach naruszenia przepisów o ochronie danych osobowych.

6. Administrator danych osobowych

Realizacja zasad przetwarzania danych osobowych należy do obowiązków **administratora danych osobowych**, którym zgodnie z art. 7 pkt 4 ustawy jest organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych. O tym, kto jest administratorem danych w sektorze publicznym decydują przepisy szczególne.

Administratorem danych osobowych uczniów i ich rodziców lub opiekunów prawnych, nauczycieli i innych pracowników szkoły jest **szkoła.** Oznacza to, że kierujący i reprezentujący ją **dyrektor szkoły zobowiązany jest zapewnić w kierowanej przez siebie placówce zgodne z prawem przetwarzanie danych osobowych oraz ponosi odpowiedzialność za działania wszystkich osób upoważnionych do przetwarzania danych.**

W świetle przepisów ustawy o ochronie danych osobowych – nowelizacja obowiązująca od 1 stycznia 2015 r. - administrator danych osobowych może powołać **administratora bezpieczeństwa informacji (ABI)**, którego zgłasza do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Z tą chwilą na administratorze bezpieczeństwa informacji spoczywa prawny obowiązek zapewnienia przestrzegania przepisów o ochronie danych osobowych, w tym za zabezpieczenie danych osobowych.

Głównym zadaniem ABI jest zapewnianie przestrzegania przepisów o ochronie danych osobowych (zgodnie z art. 36a ust. 2 pkt 1 ustawy), w szczególności przez:

1. sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
2. nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, oraz przestrzegania zasad w niej określonych,
3. zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Kolejnym zadaniem ABI jest prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych (zgodnie z art. 36a ust. 2 pkt 2 ustawy o ochronie danych osobowych).

7. Powierzenie przetwarzania danych

Na podstawie art. 31 ust. 1 ustawy administrator danych (np. pracodawca) może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. Niezbędnymi elementami tej umowy jest określenie celu, w jakim podmiot, któremu powierzono przetwarzanie danych, może je przetwarzać, oraz zakresu powierzonych do przetwarzania danych. Podmiot ten może bowiem przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie. Powierzenie przetwarzania danych na podstawie umowy, o której stanowi art. 31 ustawy, w określonym w niej celu, jest działaniem prawnie dopuszczalnym i nie stanowi nieuprawnionego udostępnienia danych przez ich administratora innemu podmiotowi. Powierzenie przetwarzanych danych nie wymaga zgody osoby, której dane dotyczą. Stosownie do art. 31 ust. 3 ustawy podmiot podejmujący się przetwarzania danych na podstawie umowy powierzenia jest zobowiązany zastosować środki zabezpieczające powierzony zbiór danych, gdyż w zakresie zabezpieczenia danych osobowych podmiot ten ponosi odpowiedzialność jak administrator danych. Musi zatem dbać o to, aby powierzone mu dane osobowe nie dostały się w ręce osób nieupoważnionych bądź nie zostały uszkodzone lub zniszczone. 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.

8. Zabezpieczenie danych osobowych

Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem (art. 36 ust. 1 ustawy). Administrator prowadzi dokumentację opisującą sposób przetwarzania danych oraz zastosowane środki techniczne i organizacyjne, a także ewidencję osób upoważnionych do ich przetwarzania. Jeśli uzna za wskazane, może też powołać administratora bezpieczeństwa informacji (ABI), który będzie odpowiedzialny za zapewnienie przestrzegania przepisów o ochronie danych osobowych w działalności szkoły i prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych. Do przetwarzania danych, o ile tak zdecyduje ich administrator, mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez

administratora (art. 37 ustawy). Osoby te są zobowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia (art. 39 ust. 2 ustawy).

Podsumowując, szkoła, jako administrator danych osobowych zobowiązana jest do:

a) przetwarzania danych zgodnie z prawem, w tym z przepisami z zakresu ochrony danych osobowych, jak i przepisami odrębnymi, szczególnymi z zakresu szeroko rozumianego sektora oświaty;

b) spełnienia wobec osób, których dane dotyczą, obowiązku informacyjnego, o którym mowa w art. 24 (gdy dane są zbierane bezpośrednio od tych osób) lub w art. 25 ustawy (gdy dane zbierane są z innych źródeł), o ile nie zachodzą wyjątki przewidziane ust. 2 powołanych artykułów ustawy; zabezpieczenia danych osobowych poprzez zastosowanie odpowiednich środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w taki sposób, aby nie były udostępniane osobom nieupoważnionym, zabrane przez osobę nieuprawnioną, a także by były zabezpieczone przed uszkodzeniem, zniszczeniem lub utratą;

c) zgłoszenia zbioru danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 i 1a ustawy. W szczególności obowiązkowi rejestracji zbiorów danych osobowych nie podlega administrator danych, który powołał administratora bezpieczeństwa informacji (ABI) i zgłosił go do rejestracji Generalnemu Inspektorowi, z wyjątkiem zbiorów, w których będą przetwarzane dane szczególnie chronione (art. 43 ust. 1a ustawy). Zwolnione z obowiązku zgłoszenia do rejestracji są również m.in. zbiory danych przetwarzanych w związku z zatrudnieniem u administratora danych (dotyczących kandydatów do pracy, obecnych i byłych pracowników), świadczeniem mu usług na podstawie umów cywilnoprawnych (np. umowy o dzieło, zlecenia), dotyczące osób uczących się u administratora danych (art. 43 ust. 1 pkt 4 ustawy), a także zbiory, które prowadzone są bez użycia systemu informatycznego, w których nie będą przetwarzane dane szczególnie chronione (art. 43 ust. 1 pkt 12 ustawy). Zwolnienie z obowiązku zgłoszenia do rejestracji nie obejmuje zbioru danych osób upoważnionych przez rodziców, czy opiekunów prawnych dziecka do ich odbioru ze szkoły. Powyższe przesłanki zwolnienia zbioru z obowiązku rejestracji nie będą miały zastosowania do większości zbiorów związanych z monitoringiem wizyjnym w szkołach, gdyż takie zbiory obejmują również dane osób innych niż te, które zostały wskazane w tych

przesłankach. Stąd w większości przypadków zbiory takie są zgłaszane przez placówki oświatowe do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

d) respektowania praw osób, których dane dotyczą, do kontroli przetwarzania ich danych w trybie i na zasadach określonych w rozdz. 4 ustawy, o czym była mowa powyżej.

II. 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. Monitoring wizyjny, który jest szczególną formą przetwarzania informacji o osobach, powinien zawsze mieć oparcie w przepisach **rangi ustawowej**, nie zaś rozporządzenia. Dlatego w przepisach ustaw dotyczących oświaty powinna znaleźć się regulacja szczególna zastępująca przepisy przyszłej ogólnej ustawy o monitoringu wizyjnym.

Obecnie w polskim porządku prawnym brak jest ustawy kompleksowo regulującej zagadnienia związane z monitoringiem wizyjnym. Obowiązujący w Polsce zakres prawnych podstaw instalowania i wykorzystywania monitoringu wizyjnego odnosi się jedynie do wybranych aspektów jego stosowania. Podstawy prawne do rejestracji obrazu (w niektórych przypadkach również dźwięku) mają służby związane z szeroko rozumianym bezpieczeństwem lub porządkiem publicznym, jak Policja, Straż Miejska, Straż Graniczna, Centralne Biuro Antykorupcyjne i in. Brak jest natomiast ustawowych uregulowań w tym zakresie dotyczących innych podmiotów państwowych i prywatnych, w tym osób fizycznych. W odniesieniu do podmiotów, które takich szczegółowych uregulowań nie posiadają, zastosowanie mają przepisy ustawy o ochronie danych osobowych.

Ponadto dyrektor szkoły powinien zadać sobie pytanie o **adekwatność wprowadzenia monitoringu wizyjnego do szkół, jako metody zapewnienia bezpieczeństwa w placówce.** Zgodnie z art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych, administrator danych osobowych powinien zapewnić, by przetwarzane informacje (wizerunek osoby, dane osobowe zwykłe i szczególnie chronione) i sposób wykonywania na nich operacji, były proporcjonalne

(adekwatne) do celów, w jakich mają być wykorzystywane. Dlatego też 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. Zgodnie z unijnym ogólnym rozporządzeniem o ochronie danych[1], które wejdzie w życie 25 maja 2018 r., takie oceny będą obowiązkowe w przypadku operacji przetwarzania stwarzających ryzyko dla ochrony praw i wolności podmiotów danych.

Monitoring wizyjny stwarza również ryzyko **przetwarzania danych osobowych innych osób,** które mogą znaleźć się w obszarze monitorowanym (wejścia do szkoły, jej otoczenie, jak ulice, chodniki, boiska czy place zabaw). Wobec tych osób kierownik jednostki 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 nauczycieli i innych pracowników szkoły.** Kwestia ta została omówiona w odpowiedzi na pytanie 4 poniżej.

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. Na przykład wspomniana straż miejska prowadzi monitoring uregulowany przepisami ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz. U. z 2013 r. poz. 1383 z późn. zm.).

W przypadkach nieuregulowanych przez przepisy szczególne, jako podstawę prawną przetwarzania danych osobowych w zakresie wizerunku, należy wskazać **przesłankę legalności określoną w art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych**, uznając za prawnie usprawiedliwiony cel administratora danych zapewnienie bezpieczeństwa osób i mienia w obszarze objętym monitoringiem.

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 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, Dz. Urz. UE L 119/1 z 4.5.2016 r.

Podkreślenia wymaga, że zgodnie ze stanowiskiem Trybunału Sprawiedliwości UE wyrażonym w wyroku w sprawie C-212/13 Ryneš, ochrona osób i mienia może być uznana za uzasadniony interes administratora w rozumieniu art. 7 lit. f) dyrektywy 95/46/WE oraz art. 23 ust. 1 pkt 5) ustawy o ochronie danych osobowych. **Każdorazowo musi to się jednak wiązać z poszanowaniem praw i wolności osoby obserwowanej oraz wypełnianiem obowiązków ustawowych administratora danych.**

3. Czy szkoła może zainstalować atrapy kamer monitoringu?

Stanowisko Generalnego Inspektora Ochrony Danych Osobowych w tej kwestii jest 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 poddawać w wątpliwość skuteczność i adekwatność tego narzędzia w realizacji zamierzonego celu w danych okolicznościach.

4. Czy monitoring w szkole, która jest miejscem pracy nauczycieli i innych pracowników szkoły, może zostać wykorzystany do kontroli ich pracy?

Możliwość stosowania określonych narzędzi kontroli nauczyciela czy innego pracownika szkoły co do zasady powinna być określona w ustawie, wraz z gwarancjami zabezpieczającymi pracowników przed ich nadużywaniem ze strony administratora. W myśl założeń monitoring w szkole ma służyć przede wszystkim poprawie bezpieczeństwa. Istnieć mogą także pokusy, by przy okazji był on narzędziem np. kontroli długości przerw czy opuszczania przez pracownika miejsca pracy, a także obserwacji czynności wykonywanych podczas świadczenia pracy, np. przez nauczyciela, sprzątaczkę, czy sekretarkę. W opinii GIODO niedopuszczalne jest instalowanie monitoringu w klasach, w których podczas trwania zajęć lekcyjnych to nauczyciel (nie zaś kamera monitoringu wizyjnego) sprawuje nadzór nad bezpieczeństwem uczniów i mienia. Obecnie w polskim porządku prawnym brakuje precyzyjnych przepisów, które w sposób wyczerpujący regulowałyby zagadnienia związane z wykorzystaniem nowoczesnych technik nadzoru w miejscu pracy. Natomiast zgodnie z Konstytucją RP, ustawą o ochronie danych osobowych czy Kodeksem pracy, podmioty stosujące monitoring powinny kierować się przede wszystkim zasadą adekwatności. Przewiduje ona, że pozyskiwać można jedynie te dane, które są niezbędne dla osiągnięcia wyznaczonego z góry, zgodnego z prawem celu. Innymi

słowy wymagane jest stosowanie tylko środków proporcjonalnych do celów przetwarzania danych osobowych. W przypadku monitoringu celem tym jest **zapewnienie bezpieczeństwa i porządku publicznego oraz ochrony osób i mienia,** nie zaś nadzór nad efektywnością czy wydajnością wykonywanej przez pracownika pracy. Co więcej, w art. 22[1] Kodeksu pracy (Dz. U. z 1998 r. Nr 21 poz. 94 z późn. zm.) określono zasadniczy katalog danych osobowych pracownika, które mogą być przetwarzane przez pracodawcę. **Nie ma wśród nich danych pozyskiwanych za pomocą monitoringu wizyjnego.**

5. Jakie obowiązki ma szkoła stosująca monitoring wizyjny?

Szkoła, która zainstalowała na swoim terenie system monitoringu wizyjnego, powinna 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.

Przykład klauzuli informacyjnej:

*„Monitoring prowadzony jest przez ....(tu nazwa podmiotu), w celu ...(*np. zapewnienie bezpieczeństwa i porządku publicznego oraz ochrony osób i mienia*) i obejmuje ....(dokładne wskazanie obszaru). Więcej informacji można uzyskać telefonicznie pod numerem telefonu ...., lub drogą elektroniczną .... (podanie adresu poczty elektronicznej, wskazanie strony internetowej)".*

Osoby znajdujące się 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.

Należy również pamiętać o obowiązku szkoły zgłoszenia zbioru związanego z monitoringiem wizyjnym do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

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. 24 i 25 ustawy o ochronie danych osobowych, zaś przepisy rozdziału 4 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 ustawy o ochronie danych osobowych. 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 również o celu ich instalacji i na jakich warunkach szkoła stosuje to narzędzie nadzoru. Ważne jest również poinformowanie o przysługującym osobie monitorowanej prawie do kontroli dotyczących jej danych osobowych - jako podmiotu danych w rozumieniu ustawy o ochronie danych osobowych (art. 32 ustawy).

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. **W opinii GIODO cała społeczność szkolna powinna współpracować z dyrektorem w kwestii podjęcia decyzji o uruchomieniu monitoringu wizyjnego na terenie placówki, po przeprowadzeniu oceny skuteczności tego systemu w utrzymaniu bezpieczeństwa w szkole i jego wpływu na prywatność.** 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 proporcjonalności środków do celu?

Szkoła, która zamierza wprowadzić monitoring, powinna wykazać zasadność jego stosowania, w tym **proporcjonalność tego środka do celu**, jakiemu ma służyć (poprawa bezpieczeństwa). Zasada ta dotyczy przede wszystkim decyzji, czy monitoring w istocie musi być stosowany i jakie argumenty przeważają za tym, że jest on lepszym środkiem niż inne dostępne służące bezpieczeństwu, czy 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.

9. W jakich miejscach monitoring w szkole może być zainstalowany?

Dyrektor szkoły, po przeanalizowaniu ewentualnych korzyści przemawiających za instalacją monitoringu w szkole nad jego niepożądanymi skutkami, wyrażając zgodę na montaż 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. **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, np. dyżurami nauczycieli czy pracowników szkoły.**

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 szkoły i umożliwiać śledzenie wykonywanych przez niego czynności na tym urządzeniu, jako, że monitoring nie powinien być wykorzystywany do nadzorowania wykonywania przez nauczycieli czy pracowników ich

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 określony. Jednakże biorąc pod uwagę, iż celem wdrażania monitoringu jest przeciwdziałanie szkodom na osobach i mieniu, należy przyjmować krótki czas przechowywania. Powoduje to nie tylko mniejszą ingerencję w prywatność osób obserwowanych, ale także zmniejszenie kosztów utrzymania systemu. Ponadto należy wziąć pod uwagę, że szkoły 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, jednakże nie dłużej niż jest to konieczne do zakończenia odpowiednich czynności wyjaśniających. Dlatego też, wobec braku przepisów dotyczących zasad stosowania monitoringu, w tym okresu przechowywania utrwalonych wizerunków osób, w chwili obecnej można powołać się na przepis art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych, w który wskazano, że administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby te dane były **przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania**. Okres ten powinien być raczej liczony w dniach niż w tygodniach. Należy jednocześnie pamiętać, iż nagrania dotyczące incydentów mogą być przechowywane dłużej – do czasu wyjaśnienia sprawy albo zakończenia odpowiednich postępowań.

11. Czy ustawa o ochronie danych osobowych ma zastosowanie do monitoringu?

Nie zawsze monitoring wizyjny wiąże się z przetwarzaniem danych osobowych. Ustawę o ochronie danych osobowych 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 elektronicznym nośniku. W przypadku gdy taki zestaw danych zostanie skatalogowany poprzez przyporządkowanie indeksów do fragmentów nagrań zawierających wizerunki osób, wówczas należy uznać, że jest to zbiór danych osobowych. Z danymi osobowymi mamy do czynienia także w

sytuacji, kiedy system, który jest instalowany równolegle z monitoringiem, umożliwia powiązanie konkretnych nagrań z konkretną osobą.

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 ustawie o ochronie danych osobowych za przetwarzanie uznaje się także gromadzenie danych. Dlatego **podmioty odpowiedzialne za gromadzenie i przechowywanie zapisów z kamer muszą stosować się wprost do przepisów** ustawy o ochronie danych osobowych.

12. Kto jest osobą odpowiedzialną za przetwarzanie danych osobowych pozyskanych przez monitoring?

Administrator danych osobowych – czyli szkoła - jest odpowiedzialna za zapewnienie bezpieczeństwa funkcjonowania systemu monitoringu wizyjnego i przetwarzanie danych osobowych pozyskanych tą drogą. Zgodnie z art. 7 pkt 4 ustawy, administratorem danych jest organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych. O tym, kto jest administratorem danych decydują przepisy szczególne. 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 administratora bezpieczeństwa informacji – jeśli został przez niego powołany.

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 w działalności szkół niejednokrotnie dochodzi do udostępnienia danych osobowych innym podmiotom na zasadzie zlecenia organizacji czy wykonania jakiejś czynności, np. przy prowadzeniu obsługi dzienników elektronicznych, czy całego systemu monitoringu zainstalowanego w danej szkole. Zgodnie z art. 31 ustawy o ochronie danych osobowych 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 powinna podjąć szkoła w kwestii zabezpieczenia danych osobowych pozyskanych z monitoringu?

Zgodnie z art. 36 ust. 1 ustawy o ochronie danych osobowych, szkoła jest obowiązana zastosować **środki techniczne i organizacyjne** zapewniające ochronę przetwarzanych danych odpowiednio do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinna zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Administrator danych ma więc obowiązek zabezpieczenia danych osobowych pochodzących z monitoringu wizyjnego. Obowiązek ten wiąże się z podjęciem przez szkołę (reprezentowaną przez dyrektora szkoły), jako administratora danych osobowych, odpowiednich działań organizacyjnych i technicznych.

Będzie on prowadził np. ewidencję osób upoważnionych do dostępu do systemu monitoringu wizyjnego, która powinna zawierać: imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do dostępu do systemu monitoringu wizyjnego.

Ponadto osoby, które zostaną upoważnione do dostępu do systemów monitoringu, mają obowiązek zachowania w tajemnicy 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.

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. Natomiast prawo do ochrony informacji dotyczącej osoby ujęte w art. 51 Konstytucji, 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 szkołę) 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.