ŚLĄSKI ZWIĄZEK GMIN I POWIATÓW
40-048 Katowice, ul. Tadeusza Kościuszki 43/5
tel. +48 32 25 11 021, 25 11 241
www. silesia.org.pl, email: zwiazek@silesia.org.pl
NIP: 634 10 87 850, Konto ING Bank Śląski 03 1050 1214 1000 0007 0001 3261

Katowice, dnia 22 grudnia 2021 roku

Rekomendacja 3/21

Komisja ds. Ochrony Danych Osobowych

Śląskiego Związku Gmin i Powiatów z siedzibą w Katowicach

dotyczy: zasad stosowania monitoringu wizyjnego przestrzeni publicznej i budynków (pomieszczeń użyteczności publicznej)

W celu wypracowania wspólnego stanowiska i jednolitego postępowania gmin i powiatów zrzeszonych w Śląskim Związku Gmin i Powiatów z siedzibą w Katowicach w zakresie stosowania przepisów o ochronie danych osobowych w związku z prowadzeniem monitoringu wizyjnego na terenie gmin i powiatów oraz należących do tych jednostek pomieszczeń użyteczności publicznej wskazuje się, jak poniżej.

A KONTEKST NORMATYWNY

Komisja ds. Ochrony Danych Osobowych (zwana dalej Komisją) podjęła inicjatywę przygotowania rekomendacji zawierającej podstawowe wskazania w zakresie bezpieczeństwa przetwarzania danych osobowych w związku z wykorzystaniem monitoringu wizyjnego.

Komisja zwraca uwagę, że rekomendacja nie wyczerpuje pełnego katalogu typów monitoringu, które mogą funkcjonować w jednostkach, a przetwarzanie danych oparte jest na różnych podstawach prawnych, w szczególności:

- art. 22 (2) Ustawy z dnia 26 czerwca 1974 r. Kodeks pracy: monitoring wizyjny, w celu *zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę,*
- art. 22 (3) Ustawy z dnia 26 czerwca 1974 r. Kodeks pracy: monitoring poczty elektronicznej i inne formy monitoringu (kontrola aktywności pracownika w sieci, rozmów telefonicznych, ewidencja czasu pracy przy użyciu zautomatyzowanych narzędzi, logowania w systemie GPS itp.), w celu *zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy*,
- art. 108a Ustawy z dnia 14 grudnia 2016 r. Prawo oświatowe: monitoring wizyjny placówek oświatowych, *w celu zapewnienia bezpieczeństwa uczniów i pracowników lub ochrony mienia*,
- art. 11 ust. 2 Ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych: prawo do obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych w celu *utrwalania dowodów popełnienia przestępstwa lub wykroczenia, przeciwdziałania przypadkom naruszania spokoju i porządku w miejscach publicznych, ochrony obiektów komunalnych i urządzeń użyteczności publicznej,* oparty nie o RODO, a Ustawę z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

Wdrażając powyższe formy monitoringu należy każdorazowo uwzględniać wymogi RODO (lub ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości), a także obowiązki wynikające z przepisów szczególnych. Trzeba również wziąć pod uwagę „nakładanie" się różnych celów i podstaw prawnych przetwarzania danych. Przykładem niech będzie monitoring wizyjny budynków, w którym przetwarzane są jednocześnie dane osobowe pracowników i klientów urzędów, gości, serwisantów czy dostawców.

I Przepisy prawa merytorycznego

Podstawa prawna realizacji zadania

- art. 6 ust. 1 lit e) Rozporządzenia 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 (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.), dalej **„RODO"**: *przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi*

w związku z:

- art. 9a oraz art. 50 Ustawy z dnia 8 marca 1990 r. o samorządzie gminnym
- art. 4b oraz art. 50 Ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym

Należy zaznaczyć, że powyższe przesłanki jedynie **uprawniają** administratorów danych do prowadzenia monitoringu wizyjnego w:

- obszarze przestrzeni publicznej w celu zapewnienia porządku publicznego i bezpieczeństwa obywateli oraz ochrony przeciwpożarowej i przeciwpowodziowej, za zgodą zarządzającego tym obszarem lub podmiotu posiadającego tytuł prawny do tego obszaru lub na terenie nieruchomości i w obiektach budowlanych stanowiących mienie gminy / powiatu lub jednostek organizacyjnych gminy / powiatu, a także na terenie wokół takich nieruchomości i obiektów budowlanych, jeżeli jest to konieczne do zapewnienia porządku publicznego i bezpieczeństwa obywateli lub ochrony przeciwpożarowej i przeciwpowodziowej,
- celu ochrony mienia (monitoring na terenie nieruchomości i w obiektach budowlanych stanowiących mienie gminy i na terenie wokół takich nieruchomości i obiektów budowlanych).

II Przepisy o ochronie danych osobowych

1. **Dane osobowe –** zgodnie z art. 4 pkt 1 RODO dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą") przy czym możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

2. **Przetwarzanie –** zgodnie z art. 4 pkt 2 RODO przetwarzanie danych oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie. Każdy rodzaj operacji na danych musi posiadać swe wyraźne uzasadnienie (podstawę mającą swoje źródło w art. 6 lub art. 9 RODO), a ich wykonywanie winno być ograniczone co do celu, zakresu przetwarzania, formy przetwarzania, czasu przetwarzania i przechowywania danych. Szczególnym atrybutem procesu przetwarzania jest **„rozliczalność”**, która nakłada na administratorów odpowiedzialność za przestrzeganie przepisów dot. ochrony danych i wymaga aby byli oni w stanie to wykazać.

3. **Administrator** – zgodnie z art. 4 pkt 7 RODO oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

W przypadku monitoringu wizyjnego, o którym mowa w niniejszej rekomendacji, administratorami są odpowiednio Gmina i/lub Powiat.

4. **Zasady przetwarzania danych osobowych wynikające z art 5 RODO, a zasada ochrony danych osobowych w fazie projektowania**

Administrator, który wprowadził monitoring zobligowany jest do stosowania zasad określonych w art. 5 ust. 2 RODO, chyba że w systemie monitoringu nie są przetwarzane dane osobowe[1].

Realizując proces przetwarzania danych administrator powinien już na etapie projektowania nowej czynności przetwarzania, zgodnie z art. 25 ust. 1 RODO, uwzględnić stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz **ryzyko naruszenia praw lub wolności osób fizycznych** o różnym prawdopodobieństwie wystąpienia i wadze wynikające z przetwarzania, zarówno – przy określaniu sposobów przetwarzania, jak i w czasie wykonywania czynności przetwarzania. Administrator powinien wdrożyć odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, a w przypadku niniejszego przetwarzania, minimalizacja zakresu danych. Administrator powinien również dołożyć wszelkiej staranności w celu wybrania niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą.

Komisja podkreśla konieczność indywidualnego podejścia **do każdej operacji przetwarzania danych osobowych i wdrożenia odpowiednich środków technicznych i organizacyjnych, analizując uprzednio ryzyka** dla tych czynności przetwarzania, tak aby przeciwdziałać ich zmaterializowaniu się, co w konsekwencji może prowadzić do naruszenia praw lub wolności osób fizycznych.

1)Przykładowo: kamery monitoringu zainstalowano na dużej wysokości, co uniemożliwia identyfikację jakiejkolwiek osoby na nagraniu lub przekazywanym z kamery obrazie „na żywo”

B REKOMENDACJA

Celem niniejszej rekomendacji jest wskazanie możliwych do zastosowania rozwiązań z zakresu ochrony prywatności i przetwarzania danych osobowych, a dotyczących stosowania przez gminę / powiat monitoringu wizyjnego służącego do rejestracji obrazu. Komisja zwraca uwagę, że monitoring wizyjny jest inwazyjną formą przetwarzania danych osobowych i jako taki powinien podlegać szczególnej weryfikacji przez administratora pod kątem potrzeby jego stosowania i konieczności zabezpieczenia oraz kontroli przez organy kontrolne[2]. Wdrażając system monitoringu wizyjnego, administrator powinien wziąć pod uwagę fakt, iż taka forma nadzoru niesie za sobą wiele zagrożeń dla praw i wolności osób fizycznych, w szczególności prawa do prywatności. Sposób i zakres monitoringu powinien być proporcjonalny w stosunku do założonego celu.

1. Cel przetwarzania

Przepisy prawa regulujące kwestie wykorzystania monitoringu wizyjnego w jednostkach samorządu terytorialnego takich jak gmina czy powiat określają cele i granice jego zastosowania.

Środki techniczne umożliwiające rejestrację obrazu (monitoring) mogą zostać użyte, jeżeli jest to konieczne do zapewnienia:

- **porządku publicznego, bezpieczeństwa obywateli, ochrony przeciwpożarowej, ochrony przeciwpowodziowej;**
- **ochrony mienia**[3].

Ograniczenia te nie znajdują zastosowania jeśli w systemie monitoringu wizyjnego nie są przetwarzane dane osobowe.

2. Zasadność stosowania monitoringu wizyjnego

Administrator planujący wdrożenie monitorowania wizyjnego w przestrzeni publicznej dokonuje oceny niezbędności (adekwatności) takiego rozwiązania biorąc pod uwagę także możliwość zastosowania innych, mniej ingerujących w prawo do prywatności osób rozwiązań. Ocena taka powinna dotyczyć każdego elementu systemu monitoringu czyli zasięgu każdej planowanej lub funkcjonującej kamery w celu wyeliminowania możliwości objęcia prywatnych posesji i budynków. Obserwacja i monitorowanie określonej przestrzeni jak i nagrywanie obrazu nie może bowiem naruszać podstawowych praw osób fizycznych. Komisja rekomenduje obligatoryjne dołączenie szkicu sytuacyjnego monitorowanego obszaru z zaznaczeniem zasięgu zastosowanych kamer.

Zalecamy, aby projektując systemy monitoringu ocenić czy nie zostanie naruszona równowaga pomiędzy zapewnieniem bezpieczeństwa osób lub mienia a prawem jednostki do ochrony wolności czy prywatności.

Zwracamy uwagę, że *zakres przedmiotowy stosowania monitoringu wizyjnego przez gminy i powiaty został [...] ograniczony do przestrzeni publicznej: parków, ulic, placów, skwerów, siłowni zewnętrznych itp. Z brzmienia przepisu wynika więc, że monitoring wizyjny nie może mieć zastosowania w odniesieniu do przestrzeni prywatnej. [...] gminy i powiaty nie mają w tym zakresie pełnej swobody i na stosowanie monitoringu wizyjnego muszą uzyskać zgodę zarządzającego obszarem objętym*

2) Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystywania monitoringu wizyjnego, Czerwiec 2018r.
3) co wynika z art. 50 ust. 2 ustawy o samorządzie gminnym i samorządzie powiatowym

monitoringiem lub podmiotu posiadającego tytuł prawny do takiego obszaru. Przykładem mogą być skwery osiedlowe lub siłownie zewnętrzne należące do wspólnot mieszkaniowych czy też spółdzielni mieszkaniowych[4].

Przed wprowadzeniem systemu monitoringu, administrator powinien uwzględnić także ochronę danych w fazie projektowania oraz domyślną ochronę danych dla systemów informatycznych przetwarzających nagrania, a także wykonać ocenę skutków dla ochrony danych, biorąc pod uwagę cel, zasadność i zakres oraz podstawę prawną wprowadzenia monitoringu wizyjnego.

3. Podstawa prawna przetwarzania danych

Podstawą prawną przetwarzania danych jest art. 6 ust. 1 lit e) RODO *przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi,* w związku z:

a) art. 9a oraz art. 50 Ustawy z dnia 8 marca 1990 r. o samorządzie gminnym,

b) art. 4b oraz art. 50 Ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym.

Stosowanie monitoringu w innych celach z powołaniem się na ww. przepisy jest niedopuszczalne. Dopuszczalna jest jednak możliwość zmiany celu przetwarzania, jeśli zostało to wyraźnie uregulowane w przepisach prawa, np.: przekazanie kopii nagrania funkcjonariuszom Policji, w związku z prowadzonym przez nich postępowaniem.

4. Zakres przetwarzania danych

Administrator uprawniony jest do rejestrowania jedynie sygnału wideo. W obecnym stanie prawnym nie występują podstawy do rejestracji dźwięku.

W klasycznym sposobie monitorowania, zakres przetwarzania danych w ramach stosowania monitoringu wizyjnego obejmował będzie w szczególności:

a) wizerunek,
b) cechy szczególne osób,
c) numery identyfikacyjne (np. numery tablic rejestracyjnych i numery boczne pojazdów).

Nagrania z monitoringu umożliwiają także określenie czasu i miejsca zarejestrowanych zdarzeń.

Monitoringiem nie można obejmować pomieszczeń sanitarnych, szatni, stołówek, palarni oraz obiektów socjalnych.

W sytuacji zastosowania specjalnych metod technicznych umożliwiających automatyczną analizę obrazu w celu dedukcji i szczegółowej identyfikacji osób obserwowanych, może dojść wówczas do przetwarzania danych szczególnie chronionych, o których mowa w art. 9 ust. 1 RODO, w tym danych biometrycznych. Komisja podkreśla z całą mocą, że zastosowane rozwiązania techniczne muszą być dobrane adekwatnie do potrzeb i pod tym kątem przeanalizowana powinna być konieczność zastosowania konkretnego rozwiązania.

4) Monitoring wizyjny w jednostkach samorządu terytorialnego – zagadnienia ogólne ANALIZY / KOMENTARZE - SAS 5 / 2020

5. Rejestr czynności przetwarzania danych

Przetwarzanie danych osobowych w związku z wykorzystaniem monitoringu wizyjnego wymaga udokumentowania w rejestrze czynności przetwarzania, zgodnie z wymogami wskazanymi w art. 30 RODO.

6. Analiza ryzyka i ocena skutków dla przetwarzania danych

Systematyczne monitorowanie na dużą skalę miejsc publicznie dostępnych jest operacją przetwarzania, która wymaga wykonania oceny skutków dla ochrony danych, obowiązek ten wynika wprost z art. 35 RODO.

Administrator analizując zasadność zastosowania monitoringu, powinien wziąć pod uwagę czy zgromadzone dane będą przetwarzane wyłącznie w Polsce, w ramach Unii czy też może nastąpić przekazanie danych poza EOG[5]. Podstawą wykonania oceny skutków dla ochrony danych jest przeprowadzenie analizy ryzyka naruszenia praw i wolności osób, których dane mogą być zgromadzone za pośrednictwem monitoringu. Analizę ryzyka należy poprzedzić dokładnym opisem zawierającym informacje o:

a) celu wprowadzenia monitoringu wraz z uzasadnieniem,

b) podstawie prawnej gromadzenia danych,

c) zakresie monitoringu wraz z planem sytuacyjnym zawierającym zakres widoczności kamer monitoringu wizyjnego oraz opisem kategorii osób, których dane dotyczą.

d) sposobie technicznej realizacji monitoringu, zastosowane urządzenia i systemy, podmioty realizujące zadanie monitorowania,

e) sposobie zapisywania, przechowywania danych oraz ich retencji.

Administrator, analizując ryzyka związane z zastosowaniem monitoringu bierze pod uwagę ewentualne konsekwencje dla:

- osób, których dane dotyczą;
- administratora danych przetwarzanych za pomocą monitoringu.

Analizując ryzyko należy wziąć pod uwagę źródła ryzyka i jego specyfikę oraz wagę, a także określić podatności adekwatne do zastosowanego rozwiązania, uwzględniając przy tym atrybuty ochrony danych: poufność, dostępność i integralność.

Ocenę skutków dla ochrony danych, administrator wykonuje według przyjętej w organizacji procedury oceny skutków dla przetwarzania danych zgodnie z art. 35, konsultując się z Inspektorem ochrony danych. Opinia Inspektora ochrony danych powinna zostać udokumentowana.

Ocena powinna zostać przeprowadzona pod kątem następujących aspektów:[6]

- ewentualne profilowanie i przewidywanie,

5) EOG tworzą państwa Unii Europejskiej oraz Islandia, Liechtenstein i Norwegia
6) Na podstawie Rekomendacji grupy art. 29

- zautomatyzowane podejmowanie decyzji wywołujące skutki prawne lub podobne,
- systematyczne monitorowanie,
- dane przetwarzane na dużą skalę,
- ewentualne połączenie danych z monitoringu z innymi zbiorami danych,
- dane dotyczące osób wymagających szczególnej opieki,
- innowacyjne wykorzystanie rozwiązań technologicznych lub organizacyjnych,
- przekazywanie danych do państw trzecich.

Administrator powinien również przeanalizować katalog środków zaradczych pozwalających uniknąć lub zminimalizować zidentyfikowane ryzyka dla procesów przetwarzania danych. Jeśli wykonana ocena wykaże wystąpienie wysokiego ryzyka dla ochrony danych, administrator ma obowiązek dokonać uprzednich konsultacji z Prezesem UODO. Uprzednich konsultacji dokonuje przy współudziale Inspektora ochrony danych.

Komisja rekomenduje aby ocenę skutków przeprowadzać tak wcześnie jak to jest możliwe, najlepiej na etapie planowania operacji przetwarzania danych. Ze względu na możliwe zmiany techniczne i organizacyjne powodujące, że zastosowane na etapie planowania, zabezpieczenia mogą być niewystarczające ocena powinna zostać powtórzona w założonym z góry okresie czasu.

7. Prawa podmiotów danych

Osoba, której dane dotyczą, ma prawo uzyskania od Administratora potwierdzenia czy jej dane są przez niego przetwarzane.

Jeżeli w chwili wniesienia żądania dane są nadal przetwarzane (tj. jeżeli dane są przechowywane lub nieustannie przetwarzane w jakikolwiek inny sposób) osoba, której dane dotyczą, powinna uzyskać dostęp i informacje zgodnie z art. 15 RODO[7]. Ze względu na specyfikę sposobu i kategorii przetwarzanych danych w systemach monitoringu, istnieją pewne ograniczenia w prawie dostępu:

a) nagranie rejestruje nieograniczoną liczbę osób, a podmiot danych wnioskuje o kopię danych; przekazanie nagrania może negatywnie wpłynąć na prawa innych osób, których wizerunki zostały zarejestrowane. W takich przypadkach należy zastosować odpowiednie środki techniczne w celu anonimizacji danych osobowych innych osób (np. maskowanie),

b) ze względu na liczbę zarejestrowanych osób Administrator może nie być w stanie zidentyfikować podmiotu danych; w takim przypadku może żądać doprecyzowania wniosku o dostęp do danych o szczegółowe informacje co do miejsca, daty lub godziny przebywania w obszarze monitorowanym.

Zaleca się, aby kwestię dostępu do danych z monitoringu określała stosowna procedura / regulamin (w szczególności zakresy odpowiedzialności czy uprawnień).

Jeżeli dane osobowe zawarte w nagraniach z monitoringu nie stanowią informacji publicznej nie ma możliwości udostępnienia ich w trybie ustawy z dnia 6 września 2001 r. o dostępie do informacji

7) Wytyczne 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo. Wersja 2.0 przyjęta w dniu 29 stycznia 2020 r.

publicznej. W takim przypadku należy odmówić udostępnienia lub udostępnić w taki sposób aby nie doszło do ujawnienia danych osób trzecich (np. poprzez anonimizację danych).

8. Obowiązek informacyjny.

Administrator realizuje obowiązek informacyjny zgodnie z art. 13 RODO oraz oznacza obszar monitorowany zgodnie z wymogami wskazanymi w akcie prawnym, który uprawnia go do stosowania monitoringu.

Komisja rekomenduje aby klauzule informacyjne zostały zamieszczone na stronach internetowych gmin i powiatów oraz w Biuletynach Informacji Publicznej tych podmiotów. Wejście na teren obszaru monitorowanego powinno zostać odpowiednio oznaczone tablicami informacyjnymi jednoznacznie informującymi o monitorowaniu przestrzeni np. „Obiekt monitorowany" i/lub znak słowno-graficzny czy piktogram.

Tablice informujące o zainstalowanym monitoringu powinny być widoczne, 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. Komisja zwraca uwagę, że oznaczenia i informacje powinny znaleźć się przed strefą monitorowaną, tak aby osoba wchodząca w taką strefę miała tego świadomość i mogła zrezygnować z poruszania się po obszarze monitorowanym[8] lub odpowiednio dostosować swoje zachowanie.

Przedmiotowa informacja przed wejściem w strefę monitoringu powinna zawierać co najmniej informacje o tożsamości i danych kontaktowych administratora, celach stosowania monitoringu oraz informacje o prawach przysługujących podmiotowi, którego dane będę przetwarzane po wejściu w monitorowaną strefę, a także informacje okresie przechowywania nagrań z monitoringu. Brak wskazania okresu retencji powoduje, że osoba wchodząca w strefę monitorowaną może przypuszczać, że obraz rejestrowany jest w czasie rzeczywistym i nie zapisuje się.

W ramach pierwszego etapu informowania o stosowanym monitoringu, powinna znaleźć się również informacja, że pełna treść klauzuli informacyjnej dostępna jest na stronie www. bądź innym łatwo dostępnym miejscu, gdzie osoba której wizerunek jest przetwarzany może się zapoznać z jej treścią[9].

9. Upoważnienie do przetwarzania danych osobowych

Administrator powinien:

a) zadbać o upoważnienie do przetwarzania danych osobowych osób mających dostęp do zapisów monitoringu,

b) w zakresie dostępu do danych, stosować zasadę minimalizacji. Dostęp do danych powinien zostać ograniczony wyłącznie do grupy osób zaangażowanych w realizację celu oraz do zakresu przypisanego każdej z nich.

8) Ibid.
9) Ibid.

10. Powierzenie przetwarzania danych

W przypadku powierzenia wykonania czynności przetwarzania podmiotowi zewnętrznemu względem administratora konieczne jest zawarcie stosownej umowy powierzenia przetwarzania danych osobowych lub porozumienia administracyjnego[10], regulujących zasady przetwarzania danych także po zakończeniu realizacji zadania. W szczególności, gdy zleca się serwis lub konserwację systemów monitoringu. Istotną kwestią jest zapewnienie dostępności i integralności danych jeśli podmiot przetwarzający przechowuje dane, nawet w formie zaszyfrowanej.

11. Okres przechowywania

Administrator określa czas przechowywania zapisów z monitoringu i informuje o tym okresie osoby, których dane dotyczą w sposób opisany w ust. 7. Komisja rekomenduje określenie czasu przechowywania do maksymalnie 90 dni.

12. Atrapy kamer

Zgodnie ze stanowiskiem Europejskiej Rady Ochrony Danych Osobowych, RODO nie ma zastosowania do atrap kamer, ponieważ nie dochodzi do utrwalenia danych osobowych, ani do innej formy ich przetwarzania[11].
Należy wziąć jednak pod uwagę opinie wyrażone przez NIK oraz organ nadzorczy[12], że atrapy kamer wprowadzają potencjalnie monitorowanych w błąd, dając z jednej strony poczucie ingerencji w sferę prywatności, a z drugiej mylne poczucie zwiększonego bezpieczeństwa.

13. Monitoring ukryty

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[13].

14. Monitoring „bez zapisu"

Monitoring dokonywany w czasie rzeczywistym bez nagrywania obrazu, to taki monitoring, w którym cel (np. zapewnienie bezpieczeństwa osobom lub ochrona mienia) osiągnięty zostaje dzięki bezpośredniej obserwacji osoby nadzorującej monitory. **Wydaje się, że stosowanie tego typu monitoringu nie jest możliwe na podstawie regulacji ustaw samorządowych**[14]. Niemniej jednak, zgodnie z opinią Europejskiej Rady Ochrony Danych Osobowych, monitoring bez zapisu również stanowi formę przetwarzania danych osobowych, przez co podlega postanowieniom RODO[15].

W ocenie Komisji, stosowanie „monitoringu bez zapisu" będzie najprawdopodobniej wymagało wskazania, odrębnej od przepisów samorządowych, podstawy prawnej i dokonania analizy

10) W przypadku jeżeli dane w imieniu administratora przetwarzają jego jednostki organizacyjne bez osobowości prawnej
11)Wytyczne 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo. Wersja 2.0 przyjęta w dniu 29 stycznia 2020 r.
12)Stanowisko Prezesa UODO jest w tej kwestii niezmienne - stosowanie atrap powinno być zakazane.
13) Ibid.
14) Red. Aneta Sieradzka, r.pr. Monika Wieczorek "Monitoring zgodny z RODO. Praktyczny poradnik z wzorami dla sektora publicznego i prywatnego „ Wyd. BECK, 2020
15 Wytyczne 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo. Wersja 2.0 przyjęta w dniu 29 stycznia 2020 r.

niezbędności i zasadności wdrożenia tego typu rozwiązania. Działania Administratora mogą mieć wpływ na prywatność osób, których dane dotyczą – w tym wypadku dochodzić może choćby do naruszenia prywatności. W przypadku przesyłania danych (obrazu) pomiędzy urządzeniami, co jest istotą monitoringu, dochodzić może również do przechwycenia transmisji, co dodatkowo może wpływać na ryzyko naruszenia wolności i praw osób obserwowanych. Należy zatem przyjąć i wdrożyć odpowiednie zabezpieczenia dla takiego procesu przetwarzania.

15. Przy wypracowaniu stanowiska wzięto pod uwagę

a) przepisy Rozporządzenia 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 (ogólne rozporządzenie o ochronie danych) „RODO”,

b) przepisy Ustawy z dnia 8 marca 1990 r. o samorządzie gminnym,

c) przepisy Ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym,

d) Wytyczne EROD 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo. Wersja 2.0 przyjęta w dniu 29 stycznia 2020 r.,

e) Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystywania monitoringu wizyjnego, Czerwiec 2018 r.