

A photograph of several white security cameras mounted on a metal bracket attached to a building's facade. The background shows a city street with buildings under a clear sky. The image has a blue tint.

Monitoring w organizacji a ochrona wizerunku

20 praktycznych rozwiązań

SPIS TREŚCI

Wstęp.....	2
Jaka podstawa przetwarzania danych z monitoringu	2
Komu musisz udostępnić dane z monitoringu	3
... a kiedy nie powinieneś tego robić.....	3
Czy można przekazać monitoring	4
Monitoring poza terenem firmy	5
Monitoring szatni – czy w każdym przypadku jest niedozwolony	6
Co z monitoringiem pomieszczeń związkowych	6
... i pomieszczeń, w których spożywa się posiłki	7
Serwis monitoringu – powierzenie czy udostępnienie danych.....	8
Publikacja wizerunku złodzieja – czy jest dopuszczalna	9
Zapisy dotyczące monitoringu – rola IOD	9
Monitoring w szpitalu – kto administruje danymi pacjentów	10
Nagrywanie dźwięku obok obrazu – czy to możliwe	11
Zasięg monitoringu w samorządzie.....	12
Domofon z kamerą w urzędzie – czy to monitoring	13
Geolokalizacja w regulaminie pracy.....	13
Odmienne rozwiązania monitoringu w szkołach – ale nie wszystkich	14
Ocena skutków w związku z monitoringiem	15
Czy pracownik może sprzeciwić się nagrywaniu rozmów telefonicznych	16
Nagrywanie filmu promocyjnego a monitoring	17

WSTĘP

Wykorzystywanie monitoringu wizyjnego w firmie jest czymś oczywistym. Oczywiście nie są jednak reguły jego stosowania. Należy zwrócić w tym zakresie uwagę w szczególności na ograniczenia w monitorowaniu (zmiany, które weszły w życie 4 maja 2019 r.), a także podstawy przetwarzania danych z kamer, w tym ich przekazywania innym podmiotom. Łatwo tu bowiem o błąd, który może administratora drogo kosztować. Właśnie tych kwestii dotyczą rozwiązania przedstawione przez naszych Ekspertów.

JAKA PODSTAWA PRZETWARZANIA DANYCH Z MONITORINGU

Pytanie: Jaka jest podstawa przetwarzania danych w ramach monitoringu wizyjnego celem ochrony mienia?

W przypadku monitoringu wizyjnego przesłankami przetwarzania danych mogą być dla organów publicznych wypełnienie obowiązku prawnego ciążącego na administratorze lub wykonanie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. W przypadku zaś podmiotów prywatnych cele wynikające z prawnie uzasadnionych interesów realizowanych przez administratora.

Przetwarzanie danych jest dopuszczalne, jeśli jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem (art. 6 ust. 1 lit. f). Zasadniczo to na tę przesłankę powołują się administratorzy danych, którzy korzystają z monitoringu wizyjnego i w jego ramach przetwarzają dane osobowe np. klientów, gości itd.

Przesłanka uzasadnionego interesu (art. 6 ust. 1 lit. f RODO) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

W grę może wchodzić – w szczególności w przypadku organów publicznych - przesłanka z art. 6 ust. 1 lit. c (wypełnienie obowiązku prawnego ciążącego na administratorze) lub z lit. e RODO (realizacja zadania publicznego).

Zobacz także: oświadczenie o wprowadzeniu monitoringu wizyjnego

KOMU MUSISZ UDOSTĘPNIĆ DANE Z MONITORINGU ...

Pytanie: Czy konieczne jest udostępnienie danych Policji w ramach prowadzonego postępowania o kradzież mienia?

Tak, należy udostępnić wskazane dane Policji. Uprawnienie Policji do przetwarzania danych osobowych wynika z art. 20 ust. 1c ustawy o Policji. Zgodnie z nim, Policja jest uprawniona do przetwarzania informacji, w tym danych osobowych, w zakresie niezbędnym do realizacji zadań ustawowych lub wykonywania uprawnień związanych z prowadzeniem postępowań administracyjnych, realizacją czynności administracyjno-porządkowych oraz innych czynności, do przeprowadzania których funkcjonariusze Policji są uprawnieni na podstawie ustaw, w celach innych niż określone w art. 1 pkt 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

... A KIEDY NIE POWINIENIEŚ TEGO ROBIĆ

Pytanie: Czy wolno udostępnić nagranie z monitoringu do wglądu osobie, której samochód został uszkodzony przez inny pojazd (zdarzenie miało miejsce na parkingu należącym do firmy)?

Nie jest dopuszczalne nie tylko udostępnienie nagrania, ale również umożliwienie wglądu do zapisów monitoringu. Administrator może jedynie udzielić informacji, czy dane zdarzenie zostało zarejestrowane na nagraniu.

Udostępnienie danych z monitoringu osobie, która nie jest uprawniona do jego prowadzenia, nie jest zatem dopuszczalne, bowiem nie mieści się w celach przetwarzania danych z monitoringu, określonych przywołanymi przepisami. Na żądanie osoby, której samochód został uszkodzony, administrator powinien jednak zabezpieczyć nagranie na którym zostało uwidocznione zdarzenie i udostępnić to nagranie na żądanie Policji. Poszkodowany powinien zatem zwrócić się do Policji ze wskazaniem, że nagranie z monitoringu może stanowić dowód w prowadzonym postępowaniu. Dopuszczalne jest zatem jedynie udzielenie przez administratora poszkodowanemu informacji, czy monitoring zarejestrował dane zdarzenie.

CZY MOŻNA PRZEKAZAĆ MONITORING

Pytanie: Czy gmina może przekazać targowisko wraz z monitoringiem zakładowi gospodarki komunalnej?

Administrator danych osobowych jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie ustala cele i sposoby przetwarzania danych osobowych (art. 4 pkt 7 RODO).

W przypadku systemu monitoringu administratorem danych będzie ten podmiot, który m. in. podejmuje decyzję o jego wdrożeniu, zainstalował urządzenia składające się na system monitoringu, prowadzi obsługę tego systemu i posiada dostęp do tego systemu. W ten sposób bowiem podmiot ten decyduje o celach przetwarzania danych osobowych (np. zapewnienie bezpieczeństwa, ochrona mienia) oraz o sposobach przetwarzania danych (rejestracja obrazu).

W konsekwencji zmiany prawa własności urządzeń składających się na system monitoringu, która jest oczywiście prawnie dopuszczalna, obsługę systemu i dostęp do systemu monitoringu będzie miał wyłącznie zakład gospodarki komunalnej jako jego właściciel. To zakład będzie decydował o celach i sposobach przetwarzania danych osobowych w systemie. Wobec tego zakład ten należy uznać za administratora danych osobowych przetwarzanych w ramach systemu monitoringu targowiska.

MONITORING POZA TERENEM FIRMY

Pytanie: Firma stosuje monitoring zewnętrzny co jest podyktowane względami bezpieczeństwa, jak i ochrony mienia. Problem polega na tym, że niektóre kamery siłą rzeczy obejmują swoim zasięgiem obszar poza terenem firmy w tym drogi gdzie przemieszczają się osoby oraz pojazdy. Jak postąpić w takiej sytuacji?

W przypadku przetwarzania danych osobowych z monitoringu, należących do kategorii danych osobowych zwykłych, podstawę prawną dla ich przetwarzania stanowi zazwyczaj art. 6 ust. 1 lit. f RODO - a więc prawnie uzasadniony interes realizowany przez administratora. Jeżeli teraz tym prawnie uzasadnionym interesem jest w przypadku konkretnego administratora bezpieczeństwo (np. chęć ograniczenia kradzieży) to monitoringiem wizyjnym powinien być **objęty tylko ten obszar, którego obserwowanie jest niezbędne ze względu na tak określony cel.**

Nie oznacza to automatycznie konieczności ograniczenia się do własnej nieruchomości.

Monitorowanie np. ulicy i ogrodzenia frontowego może być niezbędne aby uniknąć powtarzających się dewastacji skrzynki na listy czy domofonu.

Tak więc monitorowanie przestrzeni publicznie dostępnej zasadniczo nie jest zabronione.

Inaczej jest w przypadku gdy monitoring wizyjny obejmuje też inne nieruchomości. Wówczas stałe monitorowanie balkonu sąsiada może stanowić naruszenie prywatności i trudno znaleźć usprawiedliwienie dla takiego działania. Jest też jednak cała gama sytuacji „z pogranicza”. Np. monitoring wizyjny furtki na nieruchomość sąsiednią może być usprawiedliwiony w sytuacji gdy „zakreskowanie” tego fragmentu obrazu wpływałoby negatywnie na możliwość ustalenia okoliczności przestępstwa. Na przykład w tym „zakreskowanym” miejscu może stanąć na ulicy samochód, używany do włamania. Dlatego też administrator danych musi samodzielnie wyważyć oba dobra (dobra osobiste innych oraz własny cel przetwarzania danych osobowych) i podjąć **decyzję o ewentualnym ograniczeniu monitoringu wizyjnego**, biorąc pod uwagę wskazówki podane powyżej.

MONITORING SZATNI – CZY W KAŻDYM PRZYPADKU JEST NIEDOZWOLONY

Pytanie: Czy zastosowanie monitoringu wizyjnego w celu poprawy bezpieczeństwa klientów pływalni w szatniach pływalni (szatnie z szafkami zamykane na klucze w których pozostawiają swoje rzeczy i ubrania korzystający z pływalni tuż przed przejściem do przebieralni) może być uznane za nieproporcjonalne (nieadekwatne) do celów?

Zastosowanie monitoringu w szatni jest dozwolone i usprawiedliwione koniecznością zachowania bezpieczeństwa jeżeli były potwierdzone przypadki kradzieży lub innych przestępstw. Nie dochodzi także naruszenia prywatności podmiotów danych skoro w szatnia nie służy do przebierania się (została wydzielona osobna przebieralnia, nieobjęta monitoringiem). Podstawę prawną stosowania monitoringu w takiej sytuacji stanowi art. 6 ust. 1 lit. f RODO.

CO Z MONITORINGIEM POMIESZCZEŃ ZWIĄZKOWYCH ...

Pytanie: W siedzibie firmy zainstalowany jest monitoring. Tak się składa, że widać drzwi wejściowe do pomieszczenia związków zawodowych. Czy należy przesunąć kamery, tak aby nie było widać kto do tego pomieszczenia wchodzi?

Począwszy od 4 maja 2019 r. obowiązuje regulacja, zgodnie z którą monitoring nie obejmuje pomieszczeń udostępnianych zakładowej organizacji związkowej (art. 22² § 1¹ Kodeksu pracy).

Uwaga.

Pracodawca nie ma prawa instalować monitoringu w pomieszczeniach udostępnionych zakładowej organizacji związkowej niezależnie od tego czy organizacja taka wyraziła by na to swoją zgodę czy też nie.

Jeśli monitoring, o którym mowa w pytaniu, nie obejmuje pomieszczenia wyznaczonego dla organizacji związkowej, wówczas może funkcjonować tak jak dotychczas, nawet jeśli rejestruje, kto wchodzi do tego pomieszczenia. Jeśli natomiast nagrania pozwalają choćby częściowo ujrzeć samo pomieszczenie, wówczas należy dokonać **odpowiedniego przesunięcia kamer**.

Sprawdź, jak ująć monitoring wizyjny w regulaminie pracy

... I POMIESZCZEŃ, W KTÓRYCH SPOŻYWA SIĘ POSIŁKI

Pytanie: Kamera monitoringu została zainstalowana w pomieszczeniu, w którym dyżuruje pracownik ochrony. Osoba ta spożywa w tym pomieszczeniu posiłki. Czy kamerę należy usunąć?

Monitoring pomieszczeń takich jak szatnie czy stołówki może być wprowadzony po uprzednim uzyskaniu zgody zakładowej organizacji związkowej lub przedstawicieli pracowników (art. 22² § 2 Kodeksu pracy).

Zainstalowanie kamery w dyżurce przez klienta może być podyktowane względami bezpieczeństwa. Niemniej jednak w przypadku, o którym mowa w pytaniu, powstaje problem wynikający z tego, że w pomieszczeniu dyżurki pracownik ochrony przebiera się oraz spożywa posiłki. Trudno uznać, iż pomieszczenie takie spełnia definicję szatni pracowniczej oraz jadalni. Nie zmienia to jednak faktu, że podmiot który zamontował kamerę powinien zapewnić pracownikowi pracującemu w dyżurce ochronę jego dóbr osobistych. Należy przyjąć, że zastosowanie kamery w pomieszczeniu dyżurki w której pracownik ochrony będzie się przebierał oraz spożywał posiłki powinno wiązać się z zastosowaniem technik uniemożliwiających rozpoznanie osoby która w dyżurce będzie przebywała.

Uwzględniając zatem fakt, iż pomieszczenie dyżurki niezależnie od wykonywania w nim czynności z zakresu przebierania się oraz spożywania posiłków nie powinno być kwalifikowane w kategoriach szatni pracowniczej oraz jadalni można przyjąć, że **zgoda organizacji związkowych nie będzie wymagana**. Kamery nie musimy więc usuwać.

Zobacz także: ogłoszenie o wprowadzeniu monitoringu w zakładzie pracy

SERWIS MONITORINGU – POWIERZENIE CZY UDOSTĘPNIENIE DANYCH

Pytanie: Czy z firmą serwisującą sprzęt do monitoringu wizyjnego należy zawrzeć umowę o powierzenie przetwarzania danych osobowych?

Z firmą serwisową należy zawrzeć umowę powierzenia przetwarzania danych. Powierzenie przetwarzania danych osobowych pozwala w łatwy i szybki sposób uprawnicieli do przetwarzania danych osobowych podmioty, które normalnie nie mogłyby tego robić (czyli serwis, dla którego klienci firmy będącej z kolei klientem serwisu nie wyrazili przecież zgody na przetwarzanie ich danych osobowych).

Sama „czysta” umowa serwisowa nie jest umową powierzenia danych osobowych. Należy więc albo **dodać zapisy o powierzeniu danych do samej umowy serwisowej** (w formie osobnych paragrafów lub jako załącznik do tej umowy) albo **zawrzeć odrębną umowę powierzenia przetwarzania danych**.

Warto w umowie przewidzieć zapis obligujący firmę serwisową do zapewnienia odpowiednich środków bezpieczeństwa przetwarzania danych osobowych, w szczególności na nagraniach z monitoringu. Rozwiązania te powinny chronić przed wyciekiem danych w tym ich udostępnieniem osobom nieuprawnionym.

Zobacz także: Umowa powierzenia przetwarzania danych osobowych zgodna z ogólnym rozporządzeniem o ochronie danych

PUBLIKACJA WIZERUNKU ZŁODZIEJA – CZY JEST DOPUSZCZALNA

Pytanie: W lokalu firmowym kamery monitoringu zarejestrowały kradzież. Czy administrator może opublikować wizerunek złodzieja?

Praktyka taka może zostać uznana za niedozwoloną. Wprawdzie RODO zezwala na przetwarzanie danych osobowych także bez wyraźnej zgody osoby, której dane dotyczą, jednakże publikowanie wizerunku jest dodatkowo chronione. Otóż zgodnie z przepisami art. 81 ustawy o prawie autorskim i prawach pokrewnych rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej.

Zdaniem sądu

Zgodnie z wyrokiem Sądu Apelacyjnego w Warszawie z 1 stycznia 2009 r. I ACa 22/09: „Tylko zgoda upoważnia do wykorzystania – publikowania – wizerunku osoby prywatnej. I to tylko w określonym zakresie, a nie dla innych celów, choćby nawet społecznie ważnych”.

Kolejne rozwiązania dotyczące różnych form monitorowania przedstawimy w przyszłym tygodniu.

ZAPISY DOTYCZĄCE MONITORINGU – ROLA IOD

Pytanie: Czy inspektor ochrony danych jest odpowiedzialny za zmiany regulaminu pracy dotyczące monitoringu?

Inspektor ochrony danych ma następujące zadania:

- informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

- monitorowanie 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, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;
- współpraca z organem nadzorczym;
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach (art. 39 ust. 1 RODO).

W kompetencjach inspektora nie leży zatem zmiana wewnętrznych aktów prawnych takich jak regulaminy pracy. **Za te zmiany odpowiada pracodawca jako administrator danych.**

Inspektor powinien natomiast, w ramach monitorowania przestrzegania RODO, **informować administratora o konieczności wprowadzenia zmian w tych regulaminach**, jeżeli dostrzeże, że dotychczasowe zapisy są niezgodne z RODO, w szczególności, gdy nie zapewniają wymaganego przez RODO poziomu bezpieczeństwa przetwarzania danych.

MONITORING W SZPITALU – KTO ADMINISTRUJE DANYMI PACJENTÓW

Pytanie: Kto jest administratorem danych osobowych w postaci wizerunku pacjentów – szpital, czy firma będąca właścicielem monitoringu zainstalowanego w tym szpitalu?

Odpowiedź zależy od ustalenia, kto samodzielnie określa cele przetwarzania danych osobowych w postaci wizerunku. Administratorem jest bowiem osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (art. 4 pkt 7 RODO).

Nie ulega wątpliwości, że **własny cel przetwarzania tych danych na placówka medyczna**, jest to bowiem cel tożsamy celowi wprowadzenia monitoringu (np. ochrona mienia placówki). Tym samym placówka medyczna jest administratorem. Natomiast firma, która zainstalowała monitoring może co najwyżej przetwarzać dane osobowe osób zarejestrowanych na nagraniach **w ramach świadczenia usług na rzecz placówki medycznej** tj. bieżącego monitorowania placówki (zakładając, że takie usługi są świadczone). Dlatego administratorem danych osobowych jest placówka medyczna a firma, która zainstalowała monitoring - podmiotem przetwarzającym.

NAGRYWANIE DŹWIĘKU OBOK OBRAZU – CZY TO MOŻLIWE

Pytanie: Czy na izbie przyjęć SOR w szpitalu może być zainstalowany monitoring foniczny oprócz wizyjnego? Często pacjenci awanturują się i ubliżają pracownikom a lekarz, pielęgniarka, dyspozytor oraz ratownik medyczny to funkcjonariusze publiczni, w związku z czym postępowanie takie jest karalne. Dźwięk nagrywany byłby tylko do celów dowodowych i przechowywany przez okres 2 tygodni.

Pracodawca jako organizator procesu pracy oraz strona stosunku pracy ponosząca ryzyko prowadzonej działalności ma prawo kontrolować fakt wywiązywania się przez pracowników ze swoich obowiązków. Kodeks pracy daje podstawy prawne do wprowadzenia zarówno monitoringu wizyjnego, zwanego często wideo-nadzorem, przy pomocy kamer przemysłowych. Nie jest to jednak jedyna dopuszczalna prawnie forma kontroli pracowników. Kodeks pracy dopuszcza bowiem wyraźnie kontrolę służbowej poczty elektronicznej jak również **inne formy monitoringu**.

Monitoring zakładowy, w tym instalowany na terenie szpitala jest co do zasady przewidziany w relacjach pracodawca-pracownicy, w przypadkach gdzie jego stosowanie jest niezbędne do zapewnienia bezpieczeństwa, ochrony mienia, czy informacji których ujawnienie mogłoby narazić pracodawcę na szkodę.

Możliwość stosowania dodatkowego monitoringu w postaci rejestracji dźwięków, na terenie pracodawcy w tym szpitala, nie jest zagadnieniem bezpośrednio uregulowanym. Wprawdzie jak już wskazano przepisy prawa pracy dopuszczają możliwość stosowania innych rodzajów monitoringu, niż te które są bezpośrednio w kodeksie pracy uregulowane, jednak wydaje się instalacja monitoringu w postaci rejestracji dźwięku na terenie szpitala w miejscu jakim jest szpitalny oddział ratunkowy, byłaby zbyt daleko posuniętą ingerencją w prawo do prywatności w pacjentów. Z całą pewnością monitoring

taki mógłby przyczynić się do zwiększenia bezpieczeństwa zarówno personelu, jak również samych pacjentów - mógłby bowiem działać prewencyjnie i zapobiegawczo w przypadku osób, których nadmierna aktywność mogłaby wypełniać znamiona czynów ściganych przez prawo. Z drugiej jednak strony należy mieć na względzie, że monitoring rejestrujący dźwięk, rejestrowałby nie tylko awantury z udziałem wybranych pacjentów, ale również każdy inny dźwięk w tym prywatne rozmowy pacjentów w których nierzadko mogą przewijać się dane osobowe nie tylko pacjentów ale również innych osób, w tym dane dotyczące stanu zdrowia. Dlatego wydaje się, że wprowadzenie monitoringu w postaci rejestracji dźwięków w miejscu jakim jest SOR, może być oceniane w kategoriach przekroczenia dopuszczalnych form monitoringu, w tym jako **działanie naruszające w istotny sposób prawo do prywatności osób przebywających w obszarze SOR**.

ZASIĘG MONITORINGU W SAMORZĄDZIE

Pytanie: Do urzędu wpłynęła skarga o brak szczegółowej informacji dotyczącej zasięgu kamer monitoringu wizyjnego. Czy jest ona uzasadniona? Jak szczegółowo należy określić zasięg kamer?

Gmina na podstawie art. 9a ustawy o samorządzie gminnym może stosować monitoring wizyjny jedynie w celu zapewnienia porządku publicznego i bezpieczeństwa obywateli oraz ochrony przeciwpożarowej i przeciwpowodziowej, jeśli jest to konieczne do ochrony tych wartości. Jeśli zapewnienie porządku publicznego, bezpieczeństwa obywateli lub ochrony przed pożarem i powodzią jest możliwe za pomocą innych metod, wówczas gmina nie ma podstaw do korzystania z nadzoru kamer. Zgodnie z przepisami ustawy samorządowej monitoring może być prowadzony w obszarze przestrzeni publicznej, za zgodą zarządzającego tym obszarem lub podmiotu posiadającego tytuł prawny do tego obszaru lub na terenie nieruchomości i w obiektach budowlanych stanowiących mienie gminy lub jednostek organizacyjnych gminy, a także na terenie wokół takich nieruchomości i obiektów budowlanych.

Administrator danych gromadzonych za pomocą monitoringu związany jest jak każdy inny podmiot przetwarzający dane osobowe zasadami przetwarzania danych osobowych. Musi zatem pamiętać, że dane osobowe pozyskiwane za pomocą monitoringu wizyjnego powinny być adekwatne, stosowne oraz ograniczone do tego co niezbędne do celów, w których są przetwarzane (zasada minimalizacji danych). Wobec tego **zasięg kamer powinien być określony w taki sposób, aby pozyskiwane za**

ich pomocą dane osobowe były ograniczone do tego, co niezbędne dla zapewnienia porządku publicznego, bezpieczeństwa obywateli oraz ochrony przeciwpożarowej i przeciwpowodziowej.

DOMOFON Z KAMERĄ W URZĘDZIE – CZY TO MONITORING

Pytanie: Czy system domofonu z kamerą podglądową przy bocznym wejściu do urzędu podlega pod monitoring wizyjny? Jest to wejście, którym wchodzi w dużej części pracownicy lub osoby korzystające z podejścia dla niepełnosprawnych lub matek z wózkami.

Trudno w sposób jednoznaczny sklasyfikować wskazane urządzenie w kategoriach monitoringu wizyjnego stosowanego w zakładach pracy. W sytuacji gdyby urządzenie umożliwiało nie tylko bieżący podgląd w czasie rzeczywistym tego co dzieje się w zasięgu kamery będącej częścią domofonu, ale również **rejestrację dokonywanych zapisów**, wówczas instalacja domofonu w pełni wpisywała by się pojęcie monitoringu na gruncie prawa pracy - ze wszystkimi tego konsekwencjami proceduralnymi. Innymi słowy urządzenie, które nie służy do nagrywania obrazu, nie powinno być uznane za monitoring.

Uwzględniając wątpliwości co do charakteru urządzenia najbezpieczniej będzie przyjąć, nawet w sytuacji gdy stosowaniu omawianego domofonu nie towarzyszy rejestracja i przechowywanie zapisów obrazów, iż zasadnym postępowaniem będzie poinformowanie pracowników o w kwestiach technicznych związanych z użytkowanym domofonem, w tym zawiadomienie ich, że urządzenie służy jedynie do bieżącego podglądu sytuacji jaka ma miejsce w okolicy domofonu, a nie do gromadzenia informacji i przechowywania ich na takich samych zasadach jak standardowy monitoring pracowniczy.

GEOLOKALIZACJA W REGULAMINIE PRACY

Pytanie: Czy w regulaminie pracy powinna znaleźć się informacja o stosowaniu przez pracodawcę monitoringu pojazdów służbowych? Pracownicy korzystający z samochodów służbowych wyposażonych w GPS otrzymali klauzulę informacyjną w tym zakresie, oraz wyrazili pisemną zgodę na przetwarzanie ich danych osobowych w tym informacji o geolokalizacji - w przypadku korzystania z samochodu służbowego do celów prywatnych po czasie pracy.

W sytuacji o której mowa w pytaniu pracodawca zamierza stosować zarówno uregulowane bezpośrednio w kodeksie pracy formy monitoringu - kamery, monitoring służbowej poczty elektronicznej jak również rozwiązania dodatkowe postaci technologii GPS umożliwiającej śledzenie pojazdów. Każda forma monitoringu - zarówno wynikająca bezpośrednio z kodeksu pracy jak również każda inna forma monitoringu procesu pracy powinna być uregulowana w źródłach prawa zakładowego.

Cele, zakres oraz sposób zastosowania monitoringu ustala się w układzie zbiorowym pracy lub w regulaminie pracy albo w obwieszczeniu, jeżeli pracodawca nie jest objęty układem zbiorowym pracy lub nie jest obowiązany do ustalenia regulaminu pracy. Powyższa zasada dotyczy każdej formy monitoringu jaką pracodawca zamierza wprowadzić w procesie pracy.

Przepisy prawa pracy odnoszą się bezpośrednio do okresu przetwarzania zapisów monitoringu z wykorzystaniem kamer - można je przetwarzać przez okres do 3 miesięcy od dnia nagrania. W przypadku pozostałych form monitoringu kwestia okresu przetwarzania zapisów nie jest bezpośrednio uregulowana. Jeżeli pracodawca wykaże, że dla osiągnięcia celu monitoringu dany okres przetwarzania zapisów (np. roczny) będzie niezbędny, wówczas trudno będzie to zakwestionować organom kontroli i nadzoru.

Zobacz także: Oświadczenie pracodawcy o wprowadzeniu monitoringu GPS w samochodach służbowych

ODMIENNE ROZWIĄZANIA MONITORINGU W SZKOŁACH – ALE NIE WSZYSTKICH

Pytanie: Czy odmienne zasady wprowadzania monitoringu przewidziane dla szkół i placówek oświatowych w art. 108a Prawa oświatowego mają zastosowanie do placówek niepublicznych?

Art. 108a Prawa oświatowego traktujący o monitoringu wizyjnym w szkołach i placówkach

oświatowych został umiejscowiony w rozdziale 5 ustawy "Organizacja kształcenia, wychowania i opieki w szkołach i placówkach publicznych". Jest więc oczywiste, że dotyczy on publicznych szkół i placówek oświatowych.

Jednocześnie żaden przepis prawa nie przewiduje odrębnych regulacji dotyczących monitoringu dla szkół i placówek niepublicznych jak również nie wskazuje, że art. 108a Prawa oświatowego stosuje się do tych szkół i placówek odpowiednio. Wobec powyższego monitoring w szkołach i placówkach oświatowych **nie podlega regulacji art. 108a Prawa oświatowego (w tym ograniczeniom przewidzianym w tym przepisie), lecz art. 22² Kodeksu pracy.**

Wprowadzając monitoring w szkole lub placówce niepublicznej, dyrektor nie musi informować o tym fakcie uczniów ani ich rodziców.

OCENA SKUTKÓW W ZWIĄZKU Z MONITORINGIEM

Pytanie: Czy system monitoringu wymaga przeprowadzenia oceny skutków dla ochrony danych? System nie umożliwia automatycznego rozpoznawania i służy wyłącznie do analizy zdarzeń dotyczących bezpieczeństwa mienia i osób.

Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych - DPIA (art. 35 ust. 1 RODO).

Art. 35 ust. 7 RODO wymaga aby ocena zawierała:

- systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;

- ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
- ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
- środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

Należy pamiętać, że o ile przed RODO nacisk był kładziony na spełnienie wymogów formalnych (w tym posiadanie dokumentacji, którą można było opracować raz i praktycznie o niej zapomnieć) o tyle po wejściu w życie RODO ważne jest to aby nie dochodziło do naruszeń danych osobowych. W związku z tym należy przyjąć, że zwykły monitoring wizyjny nie generuje

wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, dlatego **nie ma konieczności przeprowadzania DPIA dla takiego monitoringu**.

Więcej na ten temat w artykule: [Monitorowanie danych na dużą skalę a ocena skutków dla ochrony danych](#)

CZY PRACOWNIK MOŻE SPRZECIWIĆ SIĘ NAGRYWANIU ROZMÓW TELEFONICZNYCH

Pytanie: Pracodawca chce wprowadzić monitorowanie rozmów telefonicznych pracowników w zakresie telefonów służbowych? Czy pracownicy mają prawo się temu sprzeciwić?

Jeżeli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy, pracodawca może wprowadzić kontrolę służbowej poczty elektronicznej pracownika (monitoring poczty elektronicznej). Przepis stosuje się odpowiednio do innych form monitoringu niż określona powyżej (a więc np. monitoringu rozmów telefonicznych), jeśli ich zastosowanie jest konieczne do realizacji powyższego celu (art. 22³ § 1 i 4 Kodeksu pracy).

Dopuszczalne jest wprowadzenie w zakładzie pracy monitoringu rozmów telefonicznych, jeżeli jego stosowanie jest konieczne do zagwarantowania organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy.

Wprowadzenie monitoringu rozmów telefonicznych wymaga m.i.n. ustalenia celów, zakresu oraz sposobu zastosowania monitoringu w układzie zbiorowym pracy lub w regulaminie pracy albo w obwieszczeniu, jeżeli pracodawca nie jest objęty układem zbiorowym pracy lub nie jest obowiązany do ustalenia regulaminu pracy (art. 22³ § 3 w zw. z art. 22² § 6 Kodeksu pracy).

Pracownicy nie mogą sprzeciwić się wprowadzeniu monitoringu rozmów telefonicznych. Z drugiej strony regulamin pracy ustala pracodawca w **uzgodnieniu z zakładową organizacją związkową** reprezentującą pracowników. W razie nieuzgodnienia treści regulaminu pracy z zakładową organizacją związkową w ustalonym przez strony terminie, a także w przypadku, gdy u danego pracodawcy nie działa zakładowa organizacja związkowa, regulamin pracy ustala pracodawca (art. 104² Kodeksu pracy).

Zobacz także: oświadczenie pracodawcy o wprowadzeniu monitoringu rozmów telefonicznych

NAGRYWANIE FILMU PROMOCYJNEGO A MONITORING

Pytanie: Czy na terenie firmy można zainstalować kamery, które będą filmowały przebieg pewnego fragmentu produkcji dla celów marketingowych? Nagrywanie to trwało będzie kilka miesięcy przez całą dobę. Prawo do takiego filmowania zostało wpisane do kontraktu dotyczącego wyprodukowania określonej konstrukcji.

Wprowadzenie monitoringu zakładowego w postaci kamer powinno być związane z konkretnymi przesłankami związanymi z koniecznością zapewnienia bezpieczeństwa pracowników, ochrony mienia, kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. Cele promocyjne nie mieszczą się w zakresie uzasadnionych przesłanek wprowadzenia monitoringu wizyjnego na terenie zakładu pracy.

W przypadku **gdy rejestracja procesu produkcji nie będzie dotyczyła jednocześnie pracowników**, których można zidentyfikować na podstawie zapisu takiego monitoringu, wówczas nie ma przeciwwskazań do zastosowania kamer w celu, o którym mowa w pytaniu. Jeżeli jednak rejestracja obrazu miałaby obejmować osoby zatrudnione, z możliwością ich późniejszej identyfikacji, wówczas należy odwołać się do przepisów Kodeksu pracy, które jednak nie przewidują możliwości stosowania kamer w celach marketingowych.

Monitoring wizyjny stosowany na terenie zakładu pracy znajduje się pod kontrolą Państwowej Inspekcji Pracy. Wynika to z tego, że zasady jego funkcjonowania zostały umieszczone w podstawowym źródle prawa pracy jakim jest kodeks pracy. Tym samym inspektorzy mogą zakwestionować stosowanie monitoringu w celu niekorespondującym z celami monitoringu przewidzianymi w prawie pracy.

Podstawa prawna:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 nr 119, str. 1) – art. 4, art. 28, art. 39,
- Ustawa z 26 czerwca 1974 r. – Kodeks pracy (tekst jedn.: Dz.U. z 2019 r., poz. 1040) – art. 22², art. 22³, art. 104²,
- Ustawa z 8 marca 1990 r. o samorządzie gminnym (tekst jedn.: Dz.U. z 2019 r. poz. 506) – art. 9a,
- Ustawa z 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tekst jedn.: Dz.U. z 2019 r. poz. 1231) – art. 81.

Ustawa z 14 grudnia 2016 r. - Prawo oświatowe (Dz.U. z 2018 r. poz. 996) – art.

STOPKA REDAKCYJNA

Redaktor:	Michał Kowalski
ISBN:	978-83-269-8595-9
E-book nr:	2HH0947
Firma:	Wiedza i Praktyka sp. z o.o.
Adres:	03-918 Warszawa, ul. Łotewska 9a
Kontakt:	Telefon 22 518 29 29, faks 22 617 60 10, e-mail: <i>cok@wip.pl</i>
NIP:	526-19-92-256
Numer KRS:	0000098264 – Sąd Rejonowy dla m.st. Warszawy, Sąd Gospodarczy XIII Wydział Gospodarczy Rejestrowy. Wysokość kapitału zakładowego: 200.000 zł, Nr rejestrowy BDO: 000008579
Copyright by:	Wiedza i Praktyka sp. z o.o. Warszawa 2019

Niniejszy e-book chroniony jest prawem autorskim. Przedruk materiałów bez zgody wydawcy jest zabroniony. Zakaz nie dotyczy cytowania publikacji z powołaniem się na źródło. Wszelkie materiały zawarte w niniejszej publikacji mają charakter wyłącznie popularyzacyjno-informacyjny i nie mogą być traktowane w sposób prawnie wiążący pomiędzy Czytelnikiem a wydawcą lub redakcją. Redakcja dokłada wszelkich starań, aby informacje i dane zamieszczone w tych materiałach były poprawne merytorycznie i aktualne. Jednakże decyzja odnośnie zastosowania w szczególności określonych metod leczenia czy technik medycznych należy do podmiotu uprawnionego do wykonywania działalności w tym zakresie. Informacje zawarte w niniejszej publikacji nie mają także, w aspekcie poruszanych na jej łamach zagadnień prawnych, charakteru porady czy opinii prawnej, jako że wydawca ani redakcja nie świadczą jakichkolwiek usług prawnych. Informacje tego rodzaju nie mogą być również traktowane jako oficjalne stanowisko organów lub urzędów państwowych. Zastosowanie tych informacji w konkretnym przypadku może wymagać dodatkowych, pogłębionych konsultacji lub opinii prawnej. Wobec powyższego wydawca, redakcja, redaktorzy ani autorzy ww. materiałów nie ponoszą odpowiedzialności prawnej, w szczególności za skutki zastosowania lub wykorzystania w jakikolwiek sposób informacji zawartych w niniejszej publikacji.