



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Warszawa, dnia 8 marca 2017 r.

DOLiS/DEC- 294/17/19007, 19013

dot. [...]

DECYZJA

Na podstawie art. 104 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2016 r. poz. 23 ze zm.), oraz art. 12 pkt 2, 18 ust. 1 pkt 1, art. 22 w zw. z art. 23 ust. 1 oraz art. 26 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922) po przeprowadzeniu postępowania administracyjnego w sprawie wniosku P. E. Cz. – K. [...], w przedmiocie zbadania przez Generalnego Inspektora Ochrony Danych Osobowych zgodności przetwarzania przez W. M. z siedzibą [...], jej danych osobowych z przepisami ustawy, a w szczególności w zakresie zbadania legalności pozyskiwania jej danych osobowych na skutek zainstalowania bez zgody mieszkańców budynku przy [...]monitoringu na terenie przestrzeni wspólnej, Generalny Inspektor Ochrony Danych Osobowych,

nakazuje W. M. z siedzibą w [...], usunięcie uchybień w procesie przetwarzania danych osobowych P. E. Cz. – K. zam. w [...], poprzez zaprzestanie pozyskiwania jej danych osobowych na skutek zainstalowania monitoringu przy ul. [...] na terenie przestrzeni wspólnej.

Uzasadnienie

Do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynął wniosek P. E. Cz. – K. zam. [...], zwanej dalej Skarżącą, w przedmiocie zbadania przez Generalnego Inspektora Ochrony Danych Osobowych zgodności przetwarzania przez W. M. w [...], zwanej dalej W. M., jej danych osobowych z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922), zwaną dalej ustawą, a w szczególności w zakresie zbadania legalności pozyskiwania jej danych osobowych na skutek zainstalowania bez zgody mieszkańców budynku przy ul. [...] monitoringu na terenie przestrzeni wspólnej.

W treści przedmiotowego wniosku Skarżąca podniosła, że cyt.: „[k]amerę zostały zamontowane na elewacji budynku na podstawie uchwały, która nie precyzuje co i w jaki sposób będzie monitorowane i kto jest administratorem danych osobowych, jak długo dane są przetrzymywane i w jakim celu (...). Z umowy, którą wnioskujący otrzymali w dniu [...] marca 2016r. też nie wynika, w jaki sposób są pozyskiwane dane i czy są chronione (...). (...) Zarząd ani na zebraniu właścicieli lokali w dniu [...]03.2016r. ani przed Sądem powszechnym przed którym uchwała została zaskarżona, (SO XXV 1838/15) nie określił sposobu ochrony naszych danych osobowych. Przez długi czas sądziliśmy, że kamery te są atrapami, gdyż pojawiły się potajemnie nawet bez informacji o treści uchwały i bez jakiegokolwiek oznakowania. Z oświadczenia p. A. S. wynika, że monitoring miał być instalowany w celu ochrony trawników a nie skierowany na cały teren podwórka obejmujący dojście i dojazd do budynku (w tym wejścia do naszych mieszkań tzn. wejścia na klatki schodowe). (...). Obecnie czując się całkowicie bezkarnie i poza wszelką kontrolą W. M. wskutek uzyskanej od GODO osłony swych bezprawnych działań, W. M. informacji co jest monitorowane nie podaje, jak również, nawet przed sądem nie tłumaczy jaki sposób zabezpieczenie danych osobowych został zastosowany” [pisownia jak w oryginale].

W związku z powyższym, Skarżąca wniosła do Generalnego Inspektora Ochrony Danych Osobowych o cyt.: „o powiadomienie nas o terminie kontroli, gdyż w miarę możliwości chcielibyśmy móc w niej uczestniczyć a przede wszystkim wnosimy o stwierdzenie, że monitoring mieszkańców prowadzonych przez W. M. bez zgody i wiedzy osób inwigilowanych narusza ustawę o ochronie danych osobowych”.

Skarżąca do przedmiotowego wniosku załączyła następujące dowody: 1) projekt uchwały nr [...] z dnia [...] marca 2016 r. w sprawie przyjęcia sprawozdania finansowego zarządu nieruchomością wspólną za okres [...]01.2015 r. – [...]12.2015 r. i udzielenia Zarządowi absolutorium ze sprawowania działalności w okresie [...]01.2015 r. – [...]12.2015 r.; 2) sprawozdanie ze sprawowania zarządu nieruchomością wspólną – [...] za okres od [...]01.2015 r. do [...]12.2015 r.; 3) plan gospodarczy sprawowania zarządu nieruchomością wspólną – [...] na okres [...]01.2016 r. – [...]12.2016 r.; 4) uchwałę nr [...] z dnia 18 maja 2015 r. w sprawie zainstalowania monitoringu; 5) umowę [...]na monitoring budynku [...]; 6) pismo W. z dnia [...] maja 2015 r. do Zarządu Gospodarowania Nieruchomościami w Dzielnicy [...] m.st. Warszawy.

Generalny Inspektor przeprowadził w niniejszej sprawie postępowanie administracyjne, w toku którego ustalił, co następuje.

- 1) Skarżąca jest właścicielem nieruchomości przy ul. [...] i w związku z tym jest członkiem W. M. Ponadto jest stałym użytkownikiem tej nieruchomości, co oznacza, że permanentnie korzysta z terenów należących do przestrzeni wspólnej, w szczególności z terenów, obejmujących dojście do budynku mieszkalnego (m.in. z klatki schodowej).
- 2) Przy wejściach do klatek schodowych na terenie W. znajdują się kamery monitorujące. Skarżąca podniosła również, że kamery monitorujące są zamontowane w taki sposób, że nagrywany jest teren podwórka publicznego, należącego do [...]. W. zaś ani nie

potwierdziła ani nie zaprzeczyła temu. Z punktu widzenia niniejszej sprawy ta kwestia nie jest istotna dla rozstrzygnięcia merytorycznego.

- 3) Instalacja tego monitoringu nastąpiła na podstawie uchwały nr [...] z dnia [...] maja 2015 r. Uchwała ta została podjęta w drodze indywidualnego zbierania głosów członków W. Skarżąca o podjęciu przedmiotowej uchwały została powiadomiona drogą pocztową (potwierdzenie nadania znajduje się w aktach sprawy – karta 28).
- 4) Ww. uchwała nie określa w sposób precyzyjny celu zainstalowania monitoringu na terenie W. M. W § 1 tego dokumentu wskazane jest jedynie cyt.: „W. M. [...] postanawia zainstalować kamery monitoringu przy wejściach do klatek schodowych”.
- 5) W. M. nie uchwaliła jakiegokolwiek aktu wewnętrznego czy też regulaminu, regulującego bliżej zasady korzystania z monitoringu na terenie nieruchomości przy ul. [...]. Przede wszystkim podmiot ten nie określił okoliczności w jakich wideonadzór może być stosowany, nie określił praw i obowiązków mieszkańców ww. nieruchomości związanych z zainstalowaniem kamer.
- 6) W. M. w wyjaśnieniach udzielonych przed Generalnym Inspektorem Ochrony Danych Osobowych podniosła, że nie przetwarza danych osobowych Skarżącej, zawartych na nagraniach z kamer monitorujących, wg. żadnego kryterium.
- 7) Jednocześnie podmiot ten oświadczył organowi, że monitoring nie jest prowadzony w ramach działalności zarobkowej, zawodowej ani w celach realizacji celów statutowych. Cyt.: „jedynym celem prowadzenia monitoringu jest prewencja oraz ewentualna pomoc uprawnionym organom ścigania w ustaleniu sprawców przestępstwa, gdyby takie zdarzenie miało miejsce”.
- 8) W. M. dodatkowo wskazała, że urządzenie rejestrujące zapisy z kamer monitorujących zabezpieczone jest przed dostępem osób nieuprawnionych w pomieszczeniu zamkniętym metalowymi drzwiami z dwoma zamkami oraz kratą, zaś dostęp do ww. pomieszczenia ma wyłącznie administrator danych czyli Zarząd W. M. Nośnikiem informacji jest dysk twardy, stały. Z kolei obraz z kamer monitorujących jest przetwarzany o obiegu zamkniętym, a monitoring nie jest podłączony do żadnej sieci. Nagrania z kamer są przechowywane przez 18 dni, po czym ulegają automatycznemu skasowaniu. Właściciele nieruchomości nie mają prawa wglądu do nagrań z kamer monitoringu. Nagrania te są dostępne wyłącznie dla Zarządu W. M. oraz uprawnionych organów ścigania w celu ustalenia sprawców przestępstwa, gdyby takie zdarzenie miało miejsce.
- 9) W. M. wskazała Generalnemu Inspektorowi Ochrony Danych Osobowych, że członkowie W. M., w tym Skarżąca zostali poinformowani o tym, że zostały zainstalowane kamery poprzez przekazanie im treści ww. uchwały, a także poprzez umieszczenie na elewacji budynku czterech czytelnych tablic informacyjnych o treści: „Obiekt monitorowany”. Ponadto, podmiot ten wyjaśnił organowi, że wewnątrz każdej klatki schodowej umieszczono informację o treści: „Informujemy, że przed wejściami do klatek schodowych uruchomiony został system monitoringu. Administratorem sieci jest Zarząd W. M.”.

10) W. M. również wskazała, że m.in. Skarżąca zaskarżyła ww. uchwałę do Sądu Okręgowego w Warszawie - sygn. akt [...]. Przedmiotem powództwa i treści rozprawy sądowej była nieważność/nieistnienie Uchwały nr [...] i brak ochrony danych osobowych. W dniu [...] maja 2016 r. Sąd wydał wyrok w powyższej sprawie, którym oddalił powództwo w całości. W. nadesłała do organu odpis niniejszego wyroku (kopia wyroku w aktach sprawy).

Po zapoznaniu się z całością zgromadzonego w sprawie materiału dowodowego, Generalny Inspektor Ochrony Danych Osobowych, zważył co następuje.

Organ do spraw ochrony danych osobowych dokonał w niniejszej sprawie oceny legalności przetwarzania danych osobowych Skarżącej, na skutek zainstalowania monitoringu na terenie przestrzeni wspólnej W. M. Poza oceną organu znalazła się kwestia ważności uchwały nr [...] W. M. z dnia [...] maja 2015 r., gdyż Generalny Inspektor Ochrony Danych Osobowych mocą ustawy nie posiada kompetencji w tym zakresie.

Na wstępie niniejszych rozważań należy wskazać, że w polskim porządku prawnym brak jest przepisów odnoszących się wprost do monitoringu wizyjnego w kontekście przetwarzania danych osobowych przez Wspólnoty Mieszkaniowe. W niektórych przypadkach (np. przez Policję, Straż Graniczną, ABW) używanie systemów monitoringu (wizualnego, audiowizualnego) jest obowiązkowe zgodnie z przepisami szczególnymi – jednakże to rozwiązanie nie ma zastosowania w niniejszej sprawie. Wojewódzki Sąd Administracyjny w wyroku z dnia [...] października 2013 r., sygn. akt [...] wskazał cyt.: „Sąd zdaje sobie sprawę, że korzystanie z monitoringu rodzi coraz więcej pytań o prawny zakres ingerencji w prywatność osób fizycznych i o warunki, jakie systemy monitorujące powinny spełniać. Skutkiem stosowania monitoringu może być utrwalenie wizerunku osób fizycznych, a następnie jego przechowywanie, opracowywanie i wykorzystanie dla różnych celów. Ustawa o ochronie danych osobowych nie reguluje w sposób szczególny tych kwestii, ale nie oznacza to, że na podstawie jej przepisów Generalny Inspektor Ochrony Danych Osobowych nie może w tym zakresie prowadzić postępowanie administracyjne, a w szczególności kontrolowania przestrzegania obowiązku informacyjnego (...)”.

Do kwestii przetwarzania danych za pomocą monitoringu wizyjnego wprost odnosi się natomiast Dyrektywa Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (95/46/WE), stanowiąc w motywie 14 preambuły, że „jeżeli w ramach społeczeństwa informacyjnego ma znaczenie rozwój technik gromadzenia, przekazywania, kompilowania, rejestrowania, przechowywania i przesyłania danych dźwiękowych i obrazowych osób fizycznych, niniejsza dyrektywa powinna mieć zastosowanie do przetwarzania takich danych”. Z motywu 16 wprost natomiast wynika, iż „przetwarzanie danych dźwiękowych i obrazowych, np. w przypadku nadzoru kamer wideo, nie wchodzi w zakres niniejszej dyrektywy, jeśli dokonywane jest dla potrzeb bezpieczeństwa publicznego, obronności, bezpieczeństwa narodowego lub też w trakcie działań organów państwowych w dziedzinie prawa karnego lub innych działań nie wchodzących w zakres

prawa Wspólnoty”. Oznacza to, że rejestrowanie obrazu i dźwięku objęte jest zakresem przedmiotowym i podmiotowym Dyrektywy poza wymienionymi powyżej przypadkami.

Obowiązujące przepisy o ochronie danych osobowych w odniesieniu do monitoringu mają zastosowanie w pełnym zakresie wtedy, gdy skutek stosowania monitoringu dochodzi do utworzenia zbioru danych. Wojewódzki Sąd Administracyjny z dnia 9 kwietnia 2013 r. o sygn. II SA/Wa 211/13 wskazał, że cyt.: „[i]stota sporu w niniejszej sprawie sprowadza się do ustalenia, czy system monitoringu wizyjnego Miasta L. stanowi zbiór danych osobowych w rozumieniu ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (...) i w związku z tym, czy podlega on obowiązkowi zgłoszenia przez Prezydenta Miasta L. do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych”.

Zgodnie z art. 7 pkt 1 powołanej ustawy przez zbiór danych rozumie się każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie of tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie. Przez administratora danych rozumie się organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych (art. 7 pkt 4 ww. ustawy).

Należy przy tym mieć na uwadze, Wojewódzki Sąd Administracyjny w Warszawie w już ww. wyroku z dnia 9 kwietnia 2013 r., sygn. akt II SA/Wa 211/13 wskazał, iż „zawartość zbioru tworzyć mogą dane (informacje) wyrażone w różny sposób — słowem, dźwiękiem (np. zbiory nagranych wypowiedzi), obrazem (np. zbiory zdjęć używane do identyfikacji sprawców przestępstw), itd. Można przy tym uznać, że zbiorem danych osobowych jest zarówno zestaw danych, odnoszący się do wielu osób, jak i odnoszący się do jednej osoby”.

Zgodnie z poglądem doktryny pojęcie zbioru danych należy do podstawowych pojęć ustawy. Ustalenie jego zakresu ma zasadnicze znaczenie dla wyznaczenia zakresu stosowania całej ustawy oraz jej poszczególnych rozwiązań. W rozumieniu ustawy zbiorem danych jest zestaw danych o charakterze osobowym, posiadający własną strukturę, w którym dane są dostępne według określonych kryteriów. Nie jest natomiast istotne to, czy zestaw ten jest scentralizowany, czy rozproszony, jednolity albo podzielony funkcjonalnie bądź geograficznie. Pojęcie zbioru danych obejmuje swym zakresem zarówno zbiory zautomatyzowane, jak i niezautomatyzowane (manualne, tradycyjne). Można więc przyjąć, iż ochrona nie jest uzależniona od techniki zastosowanej przy tworzeniu czy eksploatacji zbioru. Nieistotny jest też rodzaj nośnika zbioru danych (por. J. Barta, P. Fajgielski, R. Markiewicz "Ochrona danych osobowych. Komentarz.", publ. LEX Nr 106659). Zawartość zbioru tworzyć mogą dane (informacje) wyrażone w różny sposób - słowem, dźwiękiem (np. zbiory nagranych wypowiedzi), obrazem (np. zbiory zdjęć używane do identyfikacji sprawców przestępstw) itd. Można przy tym uznać, że zbiorem danych osobowych jest zarówno zestaw danych, odnoszących się do wielu osób, jak i odnoszących się do jednej osoby (tamże).

Z kolei, w myśl art. 6 ust. 1 ustawy, za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Zgodnie z ww. definicją dane osobowe mogą przybrać różną formę, mogą to być np.: zdjęcia, filmy, zarejestrowane wizerunki. Każda informacja, niezależnie od sposobu i formy jej wyrażenia, podlegać może ocenie z punktu

widzenia pojęcia danych osobowych i każda informacja może zostać uznana za informację o charakterze osobistym. Natomiast zgodnie z art. 6 ust. 2 ustawy, osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Czynnikiemami określającymi cechy osoby będzie m.in. wizerunek osoby (cechy fizyczne), status majątkowy (cechy ekonomiczne), poglądy polityczne, religijne lub filozoficzne oraz przynależność wyznaniowa, partyjna lub związkowa (cechy te można zaliczyć do cech umysłowych, kulturowych lub społecznych, w zależności od sposobu interpretacji tych pojęć). W przypadku obserwacji i rejestracji obrazu ww. cechy są możliwe do ustalenia. Jednocześnie w myśl art. 6 ust. 3 ustawy, informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Warto w tym miejscu przywołać definicję danych osobowych zawartą w opinii nr 4/2007 z dnia 20 czerwca 2007 r. Grupy Roboczej ds. ochrony danych osobowych, ustanowionej na mocy art. 29 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (zwanej dalej Grupą Roboczą art. 29) w kontekście wideofilmowania człowieka za pomocą kamer. Zgodnie z reprezentowanym tam poglądem cyt.: „pojęcie danych osobowych obejmuje informacje dostępne w jakiegokolwiek formie, na przykład alfabetycznej, liczbowej, graficznej, fotograficznej czy akustycznej (...), w szczególności dane dźwiękowe oraz obrazowe zaliczają się do danych osobowych, jako że mogą zawierać informacje na temat osoby fizycznej”. Ponadto, w opinii tej wskazano, iż „istotnym czynnikiem pozwalającym na ocenę <wszystkich sposobów, jakimi można się posłużyć> w celu zidentyfikowania osoby jest cel przetwarzania danych przez administratora” (...), w przypadkach gdy celem przetwarzania danych jest identyfikacja osób, można przypuszczać, że administratorzy danych dysponują sposobami <jakimi można się posłużyć> w celu zidentyfikowania osoby, której dane dotyczą. Twierdzenie, że osoby nie są możliwe do zidentyfikowania, podczas gdy celem przetwarzania danych jest właśnie ich identyfikacja, zawierałoby wewnętrzną sprzeczność. Dlatego informacje takie należy uważać za dotyczące osób możliwych do zidentyfikowania, a przetwarzanie ich powinno podlegać przepisom dotyczącym ochrony danych osobowych”. W tej samej opinii Grupa Robocza, w przykładzie nr 14 dotyczącym „nadzoru wideo” wskazała, iż „celem nadzoru wideo jest zidentyfikowanie osób występujących na obrazie wideo w każdym przypadku, gdy administrator stwierdza taką potrzebę, należy uznać cały proces za przetwarzanie danych dotyczących osób możliwych do zidentyfikowania, nawet jeżeli niektóre zarejestrowane osoby nie są możliwe do zidentyfikowania w praktyce”.

W kontekście definicji danych osobowych należy również wskazać, pogląd doktryny, który stanowi, że przez informację dotyczącą osoby fizycznej należy rozumieć komunikaty (wiadomości, wypowiedzi, prezentacje) wyrażone i zapisane w jakikolwiek sposób znakami graficznymi, symbolami, w języku komputerowym, na fotografii, na taśmie magnetofonowej lub magnetowidowej itd., niezależnie od sposobu, zakresu i swobody ich udostępniania, jak też niezależnie od sposobu ich

pozyskania. Za osobę możliwą do zidentyfikowania uważana jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Numerami identyfikacyjnymi są: numer powszechnego elektronicznego systemu ewidencji ludności (PESEL); numer identyfikacji podatkowej (NIP), a także numer dokumentu tożsamości (dowodu osobistego oraz paszportu). Natomiast czynnikami określającymi cechy osoby mogą być m.in.: wygląd zewnętrzny, wzór siatkówki oka (cechy fizyczne); struktura kodu genetycznego, grupa krwi (cechy fizjologiczne); status majątkowy (cechy ekonomiczne); pochodzenie, poglądy polityczne, przekonania religijne lub filozoficzne oraz przynależność wyznaniowa, partyjna lub związkowa (cechy te można zaliczyć do cech umysłowych, kulturowych lub społecznych, w zależności od sposobu interpretacji tych pojęć). Wskazane powyżej czynniki nie wyczerpują otwartego katalogu rodzajów informacji, które mogą być przypisane konkretnej osobie fizycznej (por. J. Barta, P. Fajgielski, R. Markiewicz "Ochrona danych osobowych. Komentarz.", publ. LEX Nr 106659).

Przenosząc powyższe na grunt rozpoznawanej sprawy wskazać należy, że W. M. – wbrew jej twierdzeniu – przetwarza dane osobowe Skarżącej w postaci jej wizerunku, a także sposobu jej zachowania nagranych podczas przebywania na miejscach objętych zasięgiem monitoringu. Dane te bowiem prowadzą do jej identyfikacji. Skarżąca nie tylko jest członkiem W., ale stale użytkuje lokal przy [...]. To oznacza, że permanentnie korzysta z terenów wspólnych ww. nieruchomości, w szczególności z chodnika prowadzącego do jej mieszkania oraz z klatki schodowej. Dlatego niemożliwym jest uniknięcie nagrania jej wizerunku, który – z racji wyżej wskazanych okoliczności – pozwala w sposób niewymagający nadmiernych, kosztów, czasu i działań na zidentyfikowanie Skarżącej.

Odnosząc się zaś do kwestii, czy dane osobowe Skarżącej w zakresie wizerunku pozyskanego za pomocą nagrań z monitoringu są przetwarzane w zbiorze danych, wskazać należy, iż w niniejszej sprawie bezsporne jest, iż dane zarejestrowane z kamer wideo na terenie nieruchomości przy [...] zapisywane są według kryterium czasu, jak również według kryterium miejsca (które tożsame jest z miejscem umieszczenia kamery). Wobec powyższego uznać należy, iż system przechowujący przez 18 dni nagrania z tego obszaru zawiera zestaw danych osobowych, w tym danych osobowych Skarżącej dostępnych według określonych kryteriów, stanowi zbiór danych osobowych, w rozumieniu art. 7 pkt 1 ustawy.

Reasumując ten wątek rozważań, W. M. przetwarza dane osobowe Skarżącej w zakresie jej wizerunku pozyskanego z zainstalowanych kamer. Dlatego też w tym miejscu należy odnieść się do kwestii legalności tego procesu.

Ustawa o ochronie danych osobowych określa obowiązki administratora danych, do których należy przetwarzanie danych osobowych z zachowaniem przesłanek określonych w ustawie. Przepisem uprawniającym administratorów danych do przetwarzania zwykłych danych osób fizycznych, w tym ich udostępniania, jest art. 23 ust. 1 ustawy, zgodnie z którym, przetwarzanie danych jest dopuszczalne tylko wtedy, gdy spełniona jest jedna z przesłanek taksatywnie wskazanych w tym przepisie. Stosownie do treści powołanego przepisu, przetwarzanie danych jest

dopuszczalne wtedy, gdy: osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych (pkt 1), jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa (pkt 2), jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą (pkt 3), jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego (pkt 4), jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą (pkt 5). Katalog przesłanek wymienionych w art. 23 ww. aktu prawnego, jest zamknięty. Każda z przesłanek legalizujących proces przetwarzania danych osobowych ma charakter autonomiczny i niezależny. Oznacza to, że przesłanki te co do zasady są równoprawne, a wobec tego spełnienie co najmniej jednej z nich stanowi o zgodnym z prawem przetwarzaniu danych osobowych.

Ponadto, jak wynika z art. 26 ust. 1 ustawy, administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były: przetwarzane zgodnie z prawem (art. 26 ust. 1 pkt 1 ustawy – zasada legalności); zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu niezgodnemu z tymi celami, z zastrzeżeniami ust. 2 (art. 26 ust. 1 pkt 2 ustawy – zasada celowości); merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane (art. 26 ust. 1 pkt 3 ustawy – zasada merytorycznej poprawności i zasada adekwatności danych); przechowywane w postaci umożliwiającej identyfikację osób, których dane dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania (art. 26 ust. 1 pkt 4 ustawy – zasada ograniczenia czasowego). Przetwarzanie danych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą oraz następuje: 1) w celach badań naukowych, dydaktycznych, historycznych lub statystycznych; 2) z zachowaniem przepisów art. 23 i 25 (art. 26 ust. 2 ustawy).

Z zebranego materiału dowodowego w sprawie wynika, że Skarżąca nie wyraziła zgody na przetwarzanie jej danych osobowych przez W. M., poprzez nagrywanie jej wizerunku za pomocą kamer. Skarżąca występowała jako interwenient uboczny po stronie powodów o ustalenie nieistnienia uchwały W. M. nr [...] z dnia [...] maja 2015 r. w sprawie instalacji monitoringu, ewentualnie o stwierdzenie nieważności lub niezgodności z ustawą tej uchwały w sprawie cywilnej przed Sądem Okręgowym w Warszawie, [...]. Zatem nie zostaje spełniona przesłanka wynikająca z art. 23 ust. 1 pkt 1 ustawy.

Co zaś tyczy się przesłanki z art. 23 ust. 1 pkt 2 ustawy, to również nie ma ona zastosowania w przedmiotowej sprawie. Jak już wyżej zostało wskazane, w polskim porządku prawnym nie ma odrębnej regulacji dotyczącej stosowania monitoringu przez inne niż organy państwowe. Ponadto żaden przepis prawa, tym bardziej przepis ustawy z dnia 24 czerwca 1994 r. o własności lokali (Dz. U. z 2015 r., poz. 1892), zwanej dalej ustawą o własności lokali nie uprawnia W. M. do pozyskiwania danych osobowych członków wspólnoty, takich jak Skarżąca na skutek zainstalowania kamer video w żadnym celu.

Ponadto, Skarżąca nie zawierała ze W. umowy w przedmiocie przetwarzania danych osobowych, która dotyczyłaby zainstalowania kamer wideo, zatem pozyskiwanie jej danych osobowych w zakresie wizerunku za pomocą monitoringu wizyjnego nie jest konieczne do realizacji umowy ani nie było niezbędne do podjęcia działań przed zawarciem umowy na żądanie Skarżącej (art. 23 ust. 1 pkt 3 ustawy).

Pozyskiwanie danych osobowych Skarżącej za pomocą monitoringu przez W. M. nie jest też niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego (art. 23 ust. 1 pkt 4 ustawy). Zgodnie z poglądem doktryny, podmiotem wykonującym zadania publiczne, a zatem adresatem niniejszej przesłanki są m.in. organy państwowe lub samorządowe, państwowe lub komunalne jednostki organizacyjne, w tym również organy administracji publicznej, gdy dla realizacji swoich celów posługują się nie władczymi formami działaniami, podmioty prawa prywatnego czy nawet jednostki organizacyjne niemające osobowości prawnej, o ile tylko realizują przypisane im (zlecone) zadania publiczne (por. J. Barta, P. Fajgielski, R. Markiewicz, „Ochrona danych osobowych Komentarz”, 5. Wydanie, Warszawa 2011). W. M. zaś w ramach przyznanych jej prawem uprawnień nie wykonuje określonych przez prawo zadań realizowanych dla dobra publicznego.

W sytuacji, gdy administrator danych nie legitymuje się przesłankami wymienionymi w art. 23 ust. 1 pkt 1-4 ustawy, wtedy – w kontekście zbadania legalności przetwarzania danych osobowych - może być brana pod uwagę tylko klauzula prawnie usprawiedliwionego celu, określona w art. 23 ust. 1 pkt 5 ustawy. Administrator danych może powołać się na tą klauzulę, jeśli wykaze, iż przetwarzanie danych jest mu niezbędne dla realizacji konkretnego celu i realizacja tego celu (zgodnego z prawem) bez przetworzenia danych będzie niemożliwa. Jak wskazuje się w doktrynie cyt.: „(...) z jednej strony cel przetwarzania danych musi być usprawiedliwiony prowadzoną działalnością administratora lub odbiorcy danych, a z drugiej strony działalność ta nie może być w jakiegokolwiek mierze niezgodna z prawem, zasadami współżycia społecznego czy dobrymi obyczajami (np. zbieranie danych dla szantażu). Nie można wszakże podawać w wątpliwość istnienia usprawiedliwionego celu tylko z tego powodu, iż ma on - w całości lub części - charakter zarobkowy (...)” (J. Barta, P. Fajgielski, R. Markiewicz. Ochrona Danych Osobowych. Komentarz. LEX 2011, Wydanie V). Ponadto, art. 23 ust. 1 pkt 5 wymaga, a by przetwarzanie danych osobowych przez administratora nie naruszało praw i wolności osoby, której dane dotyczą.

W ocenie Generalnego Inspektora Ochrony Danych Osobowych w przedmiotowej sprawie W. M. jako administrator danych osobowych Skarżącej w zakresie jej wizerunku pozyskanego za pomocą kamer w żaden sposób nie wykazała organowi, dla realizacji jakiego konkretnie zgodnego z prawem celu jest jej niezbędne przetwarzanie danych osobowych Skarżącej ww. sposób. Ponadto, nie wykazała również, że realizacja tego celu bez przetworzenia danych Skarżącej w zakresie jej wizerunku będzie niemożliwa. Nie można zaś zakwalifikować cyt.: „prewencji oraz ewentualnej pomocy uprawnionym organom ścigania w ustaleniu sprawców przestępstwa, gdyby takie zdarzenie miało miejsce”, wskazanej w uchwale, jako celu prawnie usprawiedliwionego do przetwarzania danych osobowych pozyskanych z nagrań wideonadzoru. Żaden bowiem przepis prawa nie zezwala wspólnotom mieszkaniowym ograniczać sfery prywatnej człowieka w imię

przeciwdziałania ewentualnego zagrożenia. Ponadto, w toku niniejszego postępowania administracyjnego W. M. nie wykazała organowi, że decyzja o zamontowaniu kamer monitoringu jest związana z realizacją celów statutowych tego podmiotu, wręcz przeciwnie wskazała, iż w istocie realizuje cel przypisany organom ścigania i dla organów ścigania te dane pozyskuje.

Argumentem potwierdzającym niniejsze stanowisko organu jest wykładnia przepisu z art. 31 Konstytucji RP, który stanowi, że ograniczenia w korzystaniu z konstytucyjnych wolności i praw (a prawo do prywatności jest prawem konstytucyjnie chronionym w art. 47 Konstytucji RP) mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. W przypadku zaś gdy celem przetwarzania jest zapewnienie innych, również konstytucyjnych praw, to ich realizacja musi być w równowadze z prawem do wolności i prywatności. Przy tym w art. 233 ust. 1 Konstytucji RP podkreśla się, że prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym nie może podlegać ograniczeniom także w stanach nadzwyczajnych. Skoro zatem przepisy Konstytucji RP chronią przedmiotowe prawo w sytuacji zagrożenia, to tym bardziej nie mogą wprowadzać w tym zakresie ograniczeń wówczas, kiedy płynące z powyższego „korzyści” nie są wystarczające dla uznania zasadności ingerencji o takich charakterze. Zamontowanie zaś kamer przez W. M. spowodowało zaburzenie tej równowagi, gdyż dane osobowe Skarżącej są pozyskiwane w niedookreślonym celu, co niewątpliwie narusza jej prawa i wolności.

Jak wskazuje z kolei opinia Grupy Roboczej art. 29 nr 4/2004, cyt.: „w przypadku równowagi między zaangażowanymi interesami, trzeba będzie szczególnie uważnie przeanalizować, wysłuchując wcześniej zainteresowanych stron, możliwość sytuacji, w której interes osób, których dane dotyczą, zasługujący na ochronę znajdzie się w sprzeczności z instalacją systemu lub ze szczególnym sposobem postępowania w odniesieniu do przechowywania lub do innych operacji przetwarzania”. Z materiału dowodowego zebranego w niniejszej sprawie, nie wynika, aby W. M. konsultowała z mieszkańcami nieruchomości przy [...] kwestię ingerencji w ich prywatność przez podjęcie decyzji o instalacji kamer wideo w imię cyt.: „prewencji oraz ewentualnej pomocy uprawnionym organom ścigania w ustaleniu sprawców przestępstwa, gdyby takie zdarzenie miało miejsce”.

W kontekście naruszenia praw i wolności Skarżącej, powstałego w konsekwencji zainstalowania monitoringu przez W. M. podnieść należy również, że nie został wobec niej wypełniony obowiązek informacyjny. Zastrzeżenia Generalnego Inspektora Ochrony Danych budzi fakt, że ani w treści uchwały ani na tablicach informacyjnych, nie został wskazany cel uzasadniający użycie systemów video – nadzoru. Jak zostało wskazane w przywołanej już wyżej opinii Grupy Roboczej art. 29 nr 4/2004, osoby, których dane pozyskane zostały za pomocą video - nadzoru, muszą mieć świadomość faktu prowadzenia czynności video – nadzoru, muszą być również informowane dokładnie o miejscach będących pod nadzorem. Tablice informacyjne powinny być umieszczone w sposób trwały w niezbyt dużej odległości od nadzorowanych miejsc oraz powinny być widoczne i syntetyczne. Przede wszystkim muszą wskazywać cele działań nadzoru, jak również

administratora przetwarzania, zaś wymiary tablic muszą być proporcjonalne do miejsca, gdzie są umieszczone. Jednocześnie, art. 25 ust. 1 ustawy stanowi, że w przypadku zbierania danych osobowych nie od osoby, której dane dotyczą, administrator danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o: 1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku; 2) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych; 3) źródle danych; 4) prawie dostępu do treści swoich danych oraz ich poprawiania; 5) uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8 (czyli uprawnieniu do wniesienia, w przypadkach wymienionych w art. 23 ust. 1 pkt 4 i 5, pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację oraz uprawnieniu do wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, wymienionych w art. 23 ust. 1 pkt 4 i 5, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych). Materiał dowodowy nie wykazał, aby wypełniono go wobec Skarżącej w zakresie w szczególności ww. celu, prawie dostępu do treści swoich danych oraz ich poprawiania, czy w zakresie poinformowania jej o uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8 ustawy. Materiał dowodowy nie wykazał również, że W. M. spełnia przesłanki z art. 25 ust. 2 ustawy, który stanowi, że przepisu ust. 1 nie stosuje się, jeżeli: 1) przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą; 2) dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a spełnienie wymagań określonych w ust. 1 wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania; 3) dane są przetwarzane przez administratora, o którym mowa w art. 3 ust. 1 i ust. 2 pkt 1, na podstawie przepisów prawa; 4) osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1. To oznacza, że W. M. nie jest zwolniona ze spełnienia obowiązku informacyjnego wobec Skarżącej.

Z materiału dowodowego zgromadzonego w przedmiotowej sprawie nie wynika precyzyjnie ani w sposób niebudzący wątpliwości, że zamontowanie monitoringu na terenie ww. nieruchomości ma służyć na przykład ochronie własności, zdrowia, bezpieczeństwa czy życia mieszkańców nieruchomości przy [...]. Nie wynika również, jakie dokładnie dane osobowe mieszkańców nieruchomości przy ul. [...] są zbierane. Należy bowiem pamiętać, że za pomocą monitoringu mogą zostać utrwalone w formie zapisu wideo dane sensytywne w rozumieniu art. 27 ustawy, takie jak: uzależnienia mieszkańców, stan ich zdrowia, relacje z innymi ludźmi, także dotyczące preferencji seksualnych, informacje dotyczące przynależności związkowej, w tym do organizacji o charakterze politycznym oraz pochodzenie etniczne i rasowe. Jest to bardzo istotna kwestia z punktu widzenia prawa do ochrony do prywatności. Treść tablic informacyjnych oraz treść uchwały o zainstalowaniu monitoringu na terenie W. M. [...] jest zbyt lapidarna. W ocenie organu do spraw ochrony danych osobowych treść komunikatów wystosowanych przez ten podmiot, tj. cyt.: „Obiekt monitorowany” lub cyt.: „Informujemy, że przed wejściami do klatek schodowych uruchomiony został system monitoringu. Administratorem sieci jest Zarząd W. M.” w żaden sposób nie wskazuje osobom

monitorowanym w jakim zakresie dane są nagrywane, czy tylko wizerunek, czy tylko fonia, po jakim czasie dane są usuwane, i tym bardziej, jak wyżej wskazano, o celu zbierania tego rodzaju danych. Poza tym, w toku postępowania administracyjnego W. M. nie wykazała organowi, że funkcjonują w tym podmiocie jakiegokolwiek dodatkowe akty wewnętrzne, regulujące zasady korzystania z monitoringu. Lokatorzy - tacy jak Skarżąca - nie dysponują możliwościami jakiegokolwiek kontroli w zakresie gromadzenia, przechowywania, a przede wszystkim ewentualnego wykorzystania zarejestrowanych treści. Takie działanie W. M. ingeruje zatem na prawa i wolności podmiotów danych i to w zakresie nieadekwatnym do wykazanych potrzeb.

Na konieczność respektowania zasady proporcjonalności przy ingerencji w prawa i wolności podmiotów, których dane są przetwarzane na skutek zainstalowania monitoringu zwraca uwagę Grupa Robocza art. 29 we wspomnianej już opinii nr 4/2004. Pamiętać bowiem należy, że urządzenia służące do takiego monitoringu mogą być stosowane wyłącznie jako środki pomocnicze, jeśli istnieje cel rzeczywiście uzasadniający ich użycie. Systemy te mogą być stosowane, gdy inne środki prewencyjne, ochrony i/lub bezpieczeństwa, o charakterze fizycznym i/lub logicznym, niewymagające pozyskiwania obrazu (np. wykorzystywanie drzwi antywłamaniowych służące zapobieganiu aktom wandalizmu, urządzenia kontroli dostępu, wspólne systemy alarmowe), okażą się ewidentnie niewystarczające lub niemożliwe do zastosowania dla realizacji prawnie uzasadnionych celów. Innymi słowy, W. M. decydując się zamontować monitoring, powinna zastosować zasadę, według której zbierane dane muszą być adekwatne do wyznaczonego celu, z czego wynika pewnego rodzaju „obowiązek minimalizacji pozyskiwania danych”.

W. M. w wyjaśnieniach udzielonych przed organem wskazała jedynie, że celem zainstalowania monitoringu jest cyt.: „prewencja oraz ewentualna pomoc uprawnionym organom ścigania przestępstwa, gdyby takie zdarzenie miało miejsce”, co oznacza, że zbiera dane osobowe mieszkańców nieruchomości przy [...] „na zapas”. W. też nie wykazała z jakich powodów taki środek ingerencji w prawa i wolności podmiotów danych został zastosowany i jakie konkretnie inne sposoby zabezpieczenia interesów W. M. były stosowane, a okazały się nieskuteczne.

Ponadto, wskazać należy, że z ww. stwierdzenia W. M. można wnioskować, iż swoim działaniem w pewnym sensie zastępuje organy ścigania, a takiego uprawnienia nie daje jej żaden obowiązujący przepis prawa. Tak jak wyżej zostało już wskazane – organy państwowe, w tym Policja mają restrykcyjne obwarowania prawne, jeśli chodzi o stosowanie monitoringu. Z kolei w przedmiotowej sprawie W. M. w sposób dowolny, nie wykazując wyżej opisanych przesłanek, zadecydowała, że będzie przetwarzać dane osobowe mieszkańców nieruchomości przy [...], w tym Skarżącej pozyskane na skutek zainstalowania kamer.

W tej sytuacji organ do spraw ochrony danych osobowych skorzystał z uprawnień przewidzianych w art. 18 ust. 1 pkt 1 ustawy i nakazał przywrócenie stanu zgodnego z prawem, a w szczególności usunięcie uchybień poprzez zaprzestanie pozyskiwania danych osobowych Skarżącej na skutek zainstalowania monitoringu przy [...] na terenie przestrzeni wspólnej.

Ponadto, wskazać należy, że jeżeli w ocenie Skarżącej doszło do naruszenia jej dóbr osobistych przez W. M. w związku z opisaną sprawą, to zgodnie z art. 24 ustawy z dnia 23 kwietnia

1964 r. Kodeks cywilny (Dz. U. z 2016 r., poz. 380) przysługuje jej roszczenie zaniechania tego działania. W razie dokonanego naruszenia może ona także żądać, ażeby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności ażeby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Na zasadach przewidzianych w kodeksie może on również żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny. Jeżeli skutek naruszenia dobra osobistego została wyrządzona szkoda majątkowa, poszkodowany może żądać jej naprawienia na zasadach ogólnych. Przepisy powyższe nie uchybiają uprawnieniom przewidzianym w innych przepisach, w szczególności w prawie autorskim oraz w prawie wynalazczym.

W tym stanie faktycznym i prawnym Generalny Inspektor Ochrony Danych Osobowych rozstrzygnął, jak w sentencji.

Na podstawie art. 21 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922) art. 129 § 2 w zw. z art. 127 § 3 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2016 r. poz. 23 ze zm.), strona niezadowolona z niniejszej decyzji, w terminie 14 dni od dnia jej doręczenia, może zwrócić się do Generalnego Inspektora Ochrony Danych Osobowych (adres: Biuro Generalnego Inspektora Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa) z wnioskiem o ponowne rozpatrzenie sprawy.