Monitoring w placówkach medycznych z uwzględnieniem wytycznych Europejskiej Rady Ochrony Danych

Fragment

Joanna Łuczak-Tarka

Rozdział I. Prawa osób monitorowanych

1. Uwagi ogólne

W wyniku reformy europejskiego prawa ochrony danych doszło do wzmocnienia pozycji osoby, której dane dotyczą, m.in. poprzez rozbudowanie katalogu przyznanych jej uprawnień i zmodyfikowanie istniejących już na gruncie dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych oraz wprowadzenie dotkliwych sankcji finansowych w postaci administracyjnych kar pieniężnych, które mają być stosowane wobec administratorów naruszających prawa podmiotów danych (Dz.Urz. WE L Nr 281, s. 31 ze zm.)[1]. Generalnie, wśród praw podmiotowych można wskazać:

1) prawa o charakterze **informacyjnym i dostępowym** (prawo do informacji przekazywanych w związku z przetwarzaniem danych, prawo dostępu do danych, prawo do uzyskania informacji o odbiorcach, których administrator poinformował o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, prawo do przenoszenia danych);
2) prawa o charakterze **korekcyjnym i zakazowym** (prawo do sprostowania danych, prawo do usunięcia danych „prawo do bycia zapomnianym", prawo do ograniczenia

[1] Zgodnie z art. 83 ust. 5 lit. b RODO naruszenie przepisów dotyczących praw podmiotów danych, w tym także tych poddanych wideonadzorowi rodzi po stronie administratora konsekwencje w postaci **możliwości nałożenia przez organ nadzorczy administracyjnej kary pieniężnej w wysokości do równowartości 20 mln euro, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu** z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa. W oparciu o kompetencję regulacyjną państw członkowskich polski ustawodawca, na mocy art. 102 ust. 1 i 2 OchrDanychU, ograniczył wysokość możliwej do nałożenia administracyjnej kary pieniężnej do 10 000 zł, jeśli jest ona nakładana na jednostkę sektora finansów publicznych, o której mowa w art. 9 pkt 13 FinPubU, oraz do 100 000 zł, jeśli jest ona nakładana na jednostkę sektora finansów publicznych, o której mowa w art. 9 pkt 1–12 i 14 FinPubU, instytutów badawczych lub NBP.

nia przetwarzania, prawo do sprzeciwu, prawo do niepodlegania zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu)

– a w szerszym kontekście, także:

3) przysługujące podmiotom danych **środki ochrony prawnej** (tj. prawo do skargi do organu nadzorczego, prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi, podmiotowi przetwarzającemu lub organowi nadzorczemu oraz prawo do odszkodowania).

W niniejszym rozdziale zostaną omówione te z uprawnień podmiotów danych, o których mowa w przepisach rozdziału III RODO, a które będą mogły być realizowane przez pacjentów, pracowników i osoby trzecie w związku ze stosowaniem wobec nich monitoringu wizyjnego w placówkach medycznych. Wśród nich na pierwszy plan wysuwają się: prawo do informacji przekazywanych przez administratora w związku z pozyskiwaniem danych, prawo dostępu do danych oraz prawo ich usunięcia („prawo do bycia zapomnianym") i to ich realizacji poświęcono najwięcej uwagi.

2. Przejrzystość i obowiązki informacyjne administratora danych

Wśród licznych obowiązków nakładanych na administratorów mocą przepisów RODO bez wątpienia do najistotniejszych należą te o charakterze informacyjnym. Można wśród nich wyróżnić takie, które – przy ziszczeniu się określonych przesłanek – muszą być realizowane w stosunku do podmiotów danych, organu nadzorczego czy odbiorcy danych. Konieczność przekazania osobie, której dane dotyczą, informacji określonych przez prawodawcę europejskiego aktualizuje się w przypadku:

1) pozyskiwania danych osobowych – bezpośredniego, tzn. pierwotnego (art. 13 ust. 1 i 2 RODO), i pośredniego, tzn. wtórnego (art. 14 ust. 1 i 2 RODO),
2) zgłoszenia przez te osoby stosownego żądania (art. 15 ust. 1 i 2 oraz art. 19 RODO),
3) zmiany celu przetwarzania (art. 13 ust. 3 RODO),
4) naruszenia ochrony danych (art. 34 RODO).

Tak zwany obowiązek informacyjny *sensu stricto*[2], tzn. realizowany wobec osób, których dane dotyczą, w związku z pozyskiwaniem ich danych **ma charakter szczególny** w tym znaczeniu, że:

1) **jest powszechny** – obciąża wszystkie podmioty zobowiązane do przestrzegania RODO będące administratorami, a zwolnienia z tego obowiązku, mające charakter przedmiotowy, mają ograniczony zakres,
2) **jest kluczowy** z punktu widzenia osób, których dane dotyczą – w przypadku przetwarzania danych na podstawie zgody pozwala im na podjęcie świadomej decyzji co do przetwarzania dotyczących ich danych przez administratora, zaś w przy-

[2] *J. Łuczak-Tarka*, (w:) Meritum prawa ochrony danych osobowych, red. *D. Lubasz* (tekst w druku).

padku przetwarzania danych w oparciu o inne przesłanki legalizujące pozwala na kontrolowanie jego zasadności,
3) gwarantuje uzyskanie przez osoby, których dane dotyczą, podstawowych informacji o przysługujących jej uprawnieniach, **faktycznie otwierając drogę do skorzystania z nich**.

Konieczność spełnienia obowiązku informacyjnego obciąża administratora, co nie oznacza, że musi on to zadanie wykonać samodzielnie. Możliwe jest tu również przyjęcie innych rozwiązań, tzn. realizację tego zadania administrator może powierzyć podmiotowi przetwarzającemu, a w przypadku współadministrowania za realizację obowiązku informacyjnego może odpowiadać drugi ze współadministratorów, co powinno znaleźć odzwierciedlenie odpowiednio w postanowieniach umowy powierzenia czy uzgodnień między współadministratorami.

Obowiązek przekazywania określonych informacji podmiotom danych w związku z pozyskiwaniem ich danych osobowych istniał już na gruncie dyrektywy 95/46/WE. Z uwagi na konieczność transpozycji jej postanowień do prawa krajowego przepisy statuujące obowiązek informacyjny znalazły się w rozdziale 3 nieobowiązującej już ustawy z 29.8.1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922 ze zm.). Korzystając z okazji, którą niosły ze sobą prace nad RODO, prawodawca europejski zdecydował się na wprowadzenie w tym obszarze istotnych zmian, tj.:
1) katalog informacji przekazywanych osobie, której dane dotyczą, znacząco rozbudowano;
2) sposób realizacji obowiązku informacyjnego wyznacza nowo wprowadzona zasada przejrzystości,
3) za niewykonanie lub nieprawidłowe wykonanie obowiązku informacyjnego administratorom grożą sankcje finansowe w postaci administracyjnych kar pieniężnych.

Zakres informacji przekazywanej osobom, których dane dotyczą w pierwszej kolejności, uzależniony jest od sposobu pozyskiwania danych osobowych. Jeśli są one gromadzone **w sposób pierwotny**, tzn. bezpośrednio od osoby, której dane dotyczą (przy czym fakt, że dane przekazano przy wykorzystaniu narzędzi umożliwiających komunikowanie się na odległość, w tym komunikację elektroniczną, takich jak np. telefon czy e-mail, nie ma wpływu na stwierdzenie, że dane pozyskano bezpośrednio od podmiotu danych), katalog informacji, które należy umieścić w klauzuli informacyjnej, wyznaczają przepisy art. 13 ust. 1 i 2 RODO. Jeśli są one pozyskiwane **w sposób wtórny**, tzn. nie bezpośrednio od osoby, której dane dotyczą, zakres ten kształtuje art. 14 ust. 1 i 2 RODO. W przypadku stosowania w podmiotach wykonujących działalność leczniczą monitoringu wizyjnego, jako narzędzia przetwarzania danych, ich źródłem jest sam podmiot danych, mamy więc do czynienia z ich pierwotnym pozyskiwaniem[3], a zatem zakres informacji, które należy uwzględnić w treści klauzuli informacyjnej, wyznacza art. 13 ust. 1 i 2 RODO. Wśród informacji kierowanych do podmiotu danych znajdują się takie, które administrator musi umieścić w treści komunikatu zawsze, i takie, które powinny się w nim znaleźć tylko wtedy „gdy ma to zastosowanie" – **podział przedstawia tabela poniżej**.

[3] Takiej oceny nie zmienia np. fakt korzystania przez administratora z usług podmiotów zewnętrznych zarządzających monitoringiem, serwisujących sprzęt służący do nagrywania, wykonujących na zlecenie administratora obróbkę obrazu w związku z udostępnieniem nagrań na potrzeby ubezpieczyciela.

Tabela 1. Treść klauzuli informacyjnej – zakres danych

Informacje, które klauzula informacyjna musi zawierać zawsze:	Informacje, które klauzula informacyjna zawiera warunkowo – tzn. „gdy ma to zastosowanie" (lub w przypadku informacji o odbiorcach danych – jeżeli istnieją):
1) tożsamość i dane kontaktowe administratora, 2) cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania, 3) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu, 4) o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych, 5) o prawie wniesienia skargi do organu nadzorczego, 6) czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych, 7) o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.	1) tożsamość i dane kontaktowe przedstawiciela administratora[4], 2) dane kontaktowe inspektora ochrony danych, 3) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f RODO – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią, 4) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem, 5) o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz informacje o sposobach uzyskania kopii zabezpieczeń lub o miejscu ich udostępnienia, 6) o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją.

Zwrot „gdy ma to zastosowanie" należy rozumieć w ten sposób, że należące do tej kategorii informacje powinny zostać uwzględnione w treści klauzuli informacyjnej, tylko jeśli dana okoliczność związana z konkretnym administratorem i konkretnym przetwarzaniem rzeczywiście w danym przypadku występuje. Stąd też, jeśli administrator np. nie przekazuje danych do państwa trzeciego, to nie musi informować o tym fakcie podmiotów danych. Odmiennie ta kwestia została uregulowana w odniesieniu do przypadku zautomatyzowanego podejmowania decyzji, w tym profilowania, tzn. nawet jeśli administrator nie dokonuje takich operacji na danych osobowych, powinien poinformować o tym wprost. Ponadto oczywiste jest, że administrator nie może wprowadzać podmiotu danych w błąd, dlatego ze wszystkich uprawnień, które RODO przyznaje podmiotom danych, administrator powinien wskazać te, które faktycznie przysługują osobom fizycznym w związku z konkretnym przetwarzaniem ich danych, np. w związku z mającą zastosowanie podstawą przetwarzania.

[4] Art. 27 ust. 1 RODO wprowadza **obowiązek powołania na piśmie przedstawiciela administratora na terenie Unii Europejskiej**, jeśli podmiot niemający jednostek organizacyjnych w Unii przetwarza dane osób przebywających w Unii, a czynności przetwarzania wiążą się z oferowaniem towarów lub usług takim osobom w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty, lub monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii. Na marginesie podkreślić należy, że obowiązek ten – przy zaistnieniu tych samych warunków – dotyczy również podmiotu przetwarzającego.

Na ostateczną treść klauzuli informacyjnej mają również wpływ okoliczności związane z danym administratorem i to, w jaki sposób przetwarza gromadzone dane, np. czy zdecydował on o powołaniu inspektora ochrony danych, jeśli jego powołanie nie jest obligatoryjne; jakim odbiorcom dane są przekazywane; czy dane są przekazywane do państwa trzeciego. Nie dziwi więc fakt, że klauzule informacyjne administratorów przetwarzających te same kategorie danych przy wykorzystaniu tych samych narzędzi różnią się od siebie, i to nawet jeśli dane są przetwarzane w tym samych celach. W przypadku podmiotów wykonujących działalność leczniczą przetwarzających dane przy wykorzystywaniu monitoringu wizyjnego, w stosunku do znacznej ich grupy wskazać można na pewne elementy wspólne, które znajdą odbicie w treści komunikatu kierowanego do osób poddanych wideonadzorowi. Po pierwsze, na znacznej grupie tych podmiotów spoczywa **obowiązek powołania inspektora ochrony danych** na podstawie art. 37 ust. 1 RODO, zatem klauzula powinna zawierać jego dane kontaktowe. Po drugie, z uwagi na charakterystykę tych administratorów, specyfikę prowadzonej przez nie działalności oraz przepisy warunkujące dopuszczalność stosowania przez nie monitoringu **nie będzie ich dotyczył obowiązek powołania przedstawiciela na obszarze UE ani kwestia przesyłania danych do tzw. państw trzecich**[5] **oraz organizacji międzynarodowych czy zautomatyzowanego podejmowania decyzji**, w tym profilowania. Po trzecie, mając na względzie podstawy przetwarzania danych w przypadku korzystania z monitoringu w placówkach medycznych, z katalogu wszystkich uprawnień przyznanych podmiotom danych na gruncie RODO w treści klauzuli informacyjnej, jako przysługujące osobom monitorowanym podane zostaną: prawo dostępu do danych, ich usunięcia („do bycia zapomnianym") lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania oraz prawo do wniesienia skargi do Prezesa UODO. Na podobnej zasadzie, biorąc pod uwagę to, że podanie danych, w znaczeniu umożliwienia rejestracji swojego wizerunku, nie jest ani wymogiem umownym, ani warunkiem zawarcia umowy, komunikat kierowany do podmiotu danych nie będzie musiał odnosić się do tych kwestii.

Ponadto, przygotowując klauzulę informacyjną na potrzeby placówki medycznej, w związku z prowadzeniem przez nią rejestracji obrazu należy zwrócić uwagę na następujące kwestie:

1) **cel przetwarzania danych w przypadku monitoringu**:
   a) **stosowanego w miejscach ogólnodostępnych** wskazuje art. 23a ust. 1 DziałLeczU (jest nim niezbędność do zapewnienia bezpieczeństwa pacjentów oraz pracowników),
   b) **stosowanego w pokojach łóżkowych** wskazuje art. 29 WymDziałLeczR (jest nim konieczność w procesie leczenia pacjentów i dla zapewnienia im bezpieczeństwa),
   c) **stosowanego w salach izolacyjnych** wskazuje art. 18e ust. 2 ZdrPsychU (jest nim stały nadzór nad osobą z zaburzeniami psychicznymi, która przebywa w pomieszczeniu przeznaczonym do izolacji, oraz kontrola wykonania czynności związanych z tym rodzajem środka przymusu bezpośredniego);

[5] Z transferem takim moglibyśmy mieć do czynienia np. w wyniku dokonywania zapisów nagrań przy wykorzystaniu rozwiązań chmurowych.

2) **okres, przez który dane osobowe będą przechowywane**, określił ustawodawca w art. 23a ust. 2 DziałLeczU (nie dłuższy niż 3 miesiące), dopuszczając jednocześnie jego wydłużenie, jeśli pozwalają na to przepisy szczególne (np. art. 18e ust. 6 ZdrPsychU wskazuje, że nagrania z monitoringu należy przechowywać przez okres co najmniej 12 miesięcy, a nie dłużej niż przez 13 miesięcy od dnia ich zarejestrowania, chyba że zostaną one zabezpieczone jako dowód w sprawie w przypadku toczącego się postępowania).

Specyfika przetwarzania danych przez administratora będącego placówką medyczną **nasuwa pytanie o zasadność przygotowania w związku ze stosowanym monitoringiem** kilku klauzul informacyjnych skierowanych odrębnie do pracowników administratora, pacjentów i osób trzecich przebywających na terenie placówki. W zależności od danego stanu faktycznego administrator może przetwarzać przy wykorzystywaniu tego samego narzędzia różne kategorie danych, w różnych celach, w oparciu o różne podstawy przetwarzania, z czym wiążą się okoliczności, które muszą znaleźć odbicie w treści komunikatu kierowanego do osób monitorowanych, takie jak np. cel przetwarzania czy okres retencji danych. Nie należy także zapominać, że **administrator będący placówką medyczną i jednocześnie pracodawcą** może być zainteresowany zastosowaniem monitoringu wizyjnego również w miejscach znajdujących się poza obszarem ogólnodostępnym, które nie są ani pokojami łóżkowymi, ani salami izolacyjnymi (takich jak np. szpitalne laboratorium, pralnia, kuchnia, sala konferencyjna, parking) wówczas, do takiego monitoringu znajdą zastosowanie przepisy KP[6]. Dlatego też uwzględnienie faktu stosowania tzw. monitoringu pracowniczego, tzn. poza obszarem udzielania świadczeń zdrowotnych, **w ramach odrębnej klauzuli informacyjnej skierowanej do pracowników**, uznać należy za rozwiązanie trafne.

Sposób realizacji obowiązku informacyjnego determinuje wyrażona w art. 12 RODO **zasada przejrzystości** (tzw. zasada przejrzystego informowania oraz przejrzystej komunikacji)[7], zgodnie z którą każdemu podmiotowi danych należy udzielić wszelkich niezbędnych informacji i prowadzić z nim wymaganą przepisami komunikację w **zwięzłej, przejrzystej, zrozumiałej oraz łatwo dostępnej formie, jasnym i prostym językiem**, w tym w szczególności, gdy jej adresatem jest dziecko (art. 12 ust. 1 RODO). Podkreślić należy, że zasada przejrzystości jest równie istotna z punktu widzenia należytej realizacji wszystkich pozostałych obowiązków o charakterze informacyjnym, które administrator powinien spełnić wobec podmiotu danych (tzw. obowiązki informacyjne *sensu largo*)[8],

6 Wobec tego, że DziałLeczU nie wyłącza stosowania przepisów KP (poza regulacjami dotyczącymi czasu pracy pracowników podmiotów leczniczych), należy opowiedzieć się za dopuszczalnością stosowania art. 22^2 KP, regulującego cel i zakres stosowania monitoringu wizyjnego wobec pracowników.

7 Stanowi ona konsekwencję reguły rzetelności i przejrzystości przetwarzania wyrażonej w art. 5 ust. 1 lit. a RODO. Zauważyć należy, że przejrzystość jest równie istotna w przypadku korzystania przez osoby, których dane dotyczą, z innych uprawnień informacyjnych, realizowanych na podstawie art. 15–22 i 34 RODO i komunikacji z tym związanej (tzw. zasada przejrzystej komunikacji).

8 Więcej na temat zasady przejrzystej komunikacji zob. *J. Łuczak*, (w:) RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. *E. Bielak-Jomaa*, *D. Lubasz*, Warszawa 2018, s. 466–477; *P. Litwiński*, Przejrzystość oraz tryb korzystania z praw, (w:) Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz, red. *P. Litwiński*, s. 353–360; *K. Wygoda*, (w:) Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, red. *M. Sakowska-Baryła*, Warszawa 2018, s. 199–206.

podobnie jak zasada przejrzystej komunikacji, którą administrator ma obowiązek stosować przy każdym kontakcie z podmiotem danych następującym w związku z realizacją przysługujących jej praw.

Dużym wyzwaniem, któremu muszą sprostać administratorzy, jest zatem wypracowanie **nowego wzorca informacji** kierowanej do osoby, której dane dotyczą, oraz **takiego sposobu komunikowania się** z nią, w związku z realizacją przysługujących jej praw, które zarówno co do **treści, jak i formy będą odpowiadały wymogom** postawionym przez europejskiego prawodawcę. Należy więc uwzględnić, że np. w miejscach ogólnodostępnych, takich jak budynki użyteczności publicznej, odbiorcami klauzuli informacyjnej będą dzieci, osoby starsze czy słabowidzące. Administrator powinien również pamiętać, że uprawnienia związane z bezpośrednim oraz pośrednim pozyskiwaniem danych – inaczej niż w przypadku pozostałych uprawnień informacyjnych podmiotów danych – **nie są realizowane w odpowiedzi na jej wniosek czy zapytanie**. Spełnienie obowiązku przekazywania osobom fizycznym określonych informacji w związku z pozyskiwaniem ich danych osobowych wymaga więc jego aktywnej postawy.

Mając powyższe na uwadze, administrator powinien tak zaplanować sposób udostępniania klauzuli informacyjnej, aby był on skorelowany z miejscem, czasem i sposobem pozyskiwania danych, a stosowna informacja dotarła do wszystkich osób, których dane mają być zgromadzone. W obecnym stanie prawnym odpowiedzialność administratora za spełnienie obowiązku rozciąga się bowiem zarówno na **treść przekazywanego komunikatu**, który musi być kompletny (tzn. zawierać wszystkie niezbędne informacje) i poprawny (tzn. zgodny ze stanem rzeczywistym), **jego właściwą formę** (tzn. przystępną, czytelną, adekwatną do grupy adresatów), jak i **jego udostępnienie w odpowiednim momencie**.

W przypadku pierwotnego pozyskiwania danych, a więc również w wyniku stosowania monitoringu, obowiązek informacyjny, zgodnie z art. 13 ust. 1 i 2 RODO, powinien zostać spełniony **podczas ich pozyskiwania**. Z pozyskiwaniem danych przy wykorzystaniu nadzoru wizyjnego mamy do czynienia w momencie, w którym osoba fizyczna znajdzie się na terenie monitorowanym i to właśnie przed przekroczeniem granicy tego obszaru podmiot danych powinien mieć możliwość zapoznania się z informacjami dotyczącymi przetwarzania. Na takim stanowisku stanęła Europejska Rada Ochrony Danych (EROD) w swoich wytycznych dotyczących przetwarzania danych z wykorzystaniem urządzeń wideo, wskazując jednocześnie, że podmiot danych musi być w stanie ocenić, jaki dokładnie obszar został objęty monitoringiem, aby odpowiednio – móc uniknąć objęcia nadzorem wizyjnym albo pozostając na terenie monitorowanym, zachowywać się w sposób uwzględniający tę okoliczność[9].

Co ważne, prawodawca europejski nie ogranicza administratora w doborze narzędzi, którymi ma się posługiwać, realizując obowiązek informacyjny. Ogólne rozporządzenie o ochronie danych wskazuje, że informacji należy udzielać na piśmie lub w inny sposób, w tym w stosownych przypadkach elektronicznie (art. 12 ust. 1 RODO). Ponadto dopuszczalne jest wykorzystywanie standardowych znaków graficznych, których zadaniem jest

[9] Europejska Rada Ochrony Danych, Wytyczne dotyczące przetwarzania danych osobowych z wykorzystaniem urządzeń wideo 3/2019, przyjęte 29.1.2019 r. po konsultacjach publicznych, s. 26.

przedstawienie w widoczny, zrozumiały i czytelny sposób sensu przetwarzania danych (art. 12 ust. 7 RODO).

Szczególnie istotna, z punktu widzenia realizacji obowiązku informacyjnego w związku ze stosowaniem monitoringu, jest **możliwość kaskadowego (warstwowego) budowania komunikatu kierowanego do podmiotu danych**, gdyż ze względu na znaczną liczbę i charakter informacji, które administrator musi przekazać podmiotom danych, kłopotliwe jest takie oznakowanie obszaru monitorowanego, aby tekst skierowanego do nich komunikatu był dla nich łatwo dostępny i czytelny. Warstwowe klauzule informacyjne, z jednej strony, mogą być bardziej przejrzyste, gdyż z uwagi na swoją skróconą, zwięzłą formę nie przytłaczają odbiorcy liczbą podawanych informacji, z drugiej zaś, pozwalają na zwrócenie uwagi na najważniejsze okoliczności związane z przetwarzaniem. Sięgnięcie po nie pozwala, aby informacje podawane podmiotom danych były „zwięzłe, przejrzyste, zrozumiałe i łatwo dostępne", co m.in. potwierdziła w swoich wytycznych dotyczących przejrzystości Grupa Robocza Art. 29[10]. Na celowość stosowania tego typu rozwiązań pod rządami RODO w przypadku realizacji obowiązku informacyjnego związanego z monitoringiem wskazuje również Europejska Rada Ochrony Danych[11]. Obawy administratorów może jednak wzbudzać minimalny zakres danych, które powinny znaleźć się w tzw. pierwszej warstwie informacyjnej, czyli np. obok znaku graficznego wskazującego, że dany obszar jest objęty monitoringiem. Odnosząc się do tego zagadnienia, Grupa Robocza Art. 29 stanęła na stanowisku, że w pierwszej kolejności podmiotowi danych należy zawsze przekazać najistotniejsze informacje dotyczące przetwarzania, tzn. takie, które mają największy wpływ na podmiot danych oraz takie, które mogą stanowić dla niego największe zaskoczenie. Nad problematyką treści pierwszej warstwy klauzuli informacyjnej (tzw. pierwsza warstwa informacyjna) stosowanej w związku z wykorzystywaniem monitoringu pochyliła się także EROD, wskazując w sposób niewiążący, że katalog zawartych w niej informacji może obejmować te dotyczące:

1) tożsamości administratora (a tam, gdzie ma to zastosowanie – jego przedstawiciela na terenie UE[12]),
2) danych kontaktowych administratora (a tam, gdzie ma to zastosowanie – inspektora ochrony danych),
3) celu (bądź celów) przetwarzania,
4) najważniejszych praw podmiotów danych[13],
5) przetwarzania, które mają największy wpływ na podmiot danych lub mogą stanowić dla niego największe zaskoczenie, wskazując tu przykładowo: okres retencji

10 Grupa Robocza Art. 29, Wytyczne dotyczące przejrzystości na mocy rozporządzenia 2016/679, przyjęte 29.11.2017 r., ostatnio zmienione i przyjęte w dniu 11.4.2018 r., WP 260, s. 7–8, 10 oraz 16–17.

11 Europejska Rada Ochrony Danych, Wytyczne dotyczące przetwarzania danych osobowych z wykorzystaniem urządzeń wideo..., s. 26. Stosowanie warstwowych klauzul informacyjnych przez administratorów przetwarzających dane z wykorzystywaniem monitoringu wizyjnego dopuszczał również Prezes UODO – zob. Wskazówki Prezesa UODO dotyczące wykorzystywania monitoringu wizyjnego, Wersja 1 z czerwca 2018 r., s. 14 i 20, www.uodo.gov.pl/pl/220/354 (dostęp: 2.9.2019 r.).

12 Zob. art. 27 RODO.

13 Wskazano jedynie na prawo dostępu do danych oraz prawo do usunięcia danych, z jednoczesnym zaznaczeniem, że egzemplifikacja ta nie ma charakteru wyczerpującego, a także wskazaniem, w jaki sposób można uzyskać informacje o wszystkich uprawnieniach, które przysługują podmiotowi danych w związku z tym przetwarzaniem.

nagrań z monitoringu albo informacje o tym, że monitoring służy jedynie podglądowi w czasie rzeczywistym, przekazywanie danych stronom trzecim, w szczególności gdy są nimi podmioty spoza UE,

6) miejsca i sposobu uzyskania wszystkich pozostałych informacji, które zgodnie z art. 13 RODO powinny zostać przekazane podmiotowi danych, a które składają się na tzw. drugą warstwę klauzuli informacyjnej (tzw. druga warstwa informacyjna)[14].

Wobec powyższego, spotykaną niekiedy praktykę oznakowania obszaru, na którym stosowany jest monitoring wizyjny, poprzez umieszczanie przy wejściach do budynku lub części budynku (np. przy wejściu do windy lub w windzie, którą można się dostać do strefy monitorowanej) czy np. przy wjeździe na parking znaku graficznego, opatrzonego napisem: *Uwaga monitoring!* czy: *Teren monitorowany*, połączoną jedynie z podaniem miejsca, w którym można zapoznać się z tekstem klauzuli informacyjnej (np. poprzez odesłanie do strony internetowej administratora), należy uznać za naruszającą przepisy RODO. Pierwsza warstwa komunikatu kierowanego do podmiotu danych powinna służyć zarówno przekazaniu kluczowych informacji związanych z przetwarzaniem danych, jak i bezpośrednio oraz wyraźnie nawiązywać do jego drugiej warstwy. Wybór miejsca i sposobu udostępnienia uzupełniającej treści klauzuli informacyjnej należy oceniać z punktu widzenia jej dostępności dla podmiotów danych. Pamiętając, że administrator powinien zapewnić dostęp do wszystkich informacji, o których mowa w art. 13 RODO, jeszcze przed znalezieniem się przez podmioty danych w strefie monitorowanej[15], stwierdzić należy, iż może ona zostać umieszczona np. w punkcie rejestracji, przy szatni, na tablicy ogłoszeń, a możliwość zapoznania się z nią powinna zostać zagwarantowana w tej samej lokalizacji, w której stosowany jest monitoring. Możliwe jest także wykorzystywanie w celu udostępnienia drugiej warstwy klauzuli informacyjnej narzędzi cyfrowych, np. poprzez użycie kodu QR czy odesłanie do strony internetowej, jeśli tylko nie będą to jedyne instrumenty pozwalające na zapoznanie się z nią[16]. Ograniczenie możliwości uzyskania informacji uzupełniających tylko do tych źródeł stanowiłoby nieuzasadnione ograniczenie dostępu do informacji dotyczących przetwarzania, a w praktyce nawet pozbawiałoby możliwości ich uzyskania znaczną grupę podmiotów, takich jak np. osoby starsze. Podobnie krytycznie należy ocenić przyjęcie przez administratora rozwiązania umożliwiającego uzyskanie tych informacji jedynie pod numerem telefonu dostępnym w określonych godzinach, w wybrane dni tygodnia, podczas gdy wstęp na obszar monitorowany byłby możliwy także poza tymi okresami. Mimo powyższych uwag nie należy zapominać, że EROD zachęca administratorów do sięgania po nowoczesne rozwiązania technologiczne, takie jak np. geolokalizowanie kamer czy aplikacje mapujące, jeśli tylko pozwolą one uzyskać podmiotom danych bardziej szczegółowe informacje dotyczące przetwarzania[17].

Zauważyć również należy, że dodatkowe wymogi dotyczące oznakowania miejsc objętych monitoringiem mogą wprowadzać państwa członkowskie w przepisach prawa kra-

14 Europejska Rada Ochrony Danych, Wytyczne dotyczące przetwarzania danych osobowych z wykorzystaniem urządzeń wideo..., s. 26–27.
15 Tamże.
16 Tamże.
17 Tamże, s. 27.

jowego. Jako przykład należy wskazać art. 22^2 § 9 KP, zgodnie z którym pracodawca, wprowadzając monitoring na terenie zakładu pracy lub wokół zakładu pracy, musi oznaczyć pomieszczenia i teren monitorowany w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych.

W przypadku pozyskiwania danych bezpośrednio od osoby, której dane dotyczą, prawodawca europejski przewidział **tylko jedną przesłankę zwalniającą z realizacji obowiązku informacyjnego**. Jest nią posiadanie już przez podmiot danych informacji wskazanych w art. 13 ust. 1 i 2 RODO. Jeśli zatem osoba, której dane dotyczą, posiada tylko część tych informacji, na administratorze nadal spoczywa obowiązek ich przekazania w pozostałym zakresie. Negatywną przesłanką spełnienia obowiązku informacyjnego nie jest więc znaczny koszt, który administrator musi ponieść w związku z takim działaniem, ani też istotny nakład czasu i środków, które musi zaangażować[18]. Szczególne przypadki zwolnienia z obowiązku informacyjnego w przypadku zmiany celu przetwarzania danych w ramach realizacji zadania publicznego oraz w przypadku prowadzenia działalności związanej z materiałami prasowymi, działalności literackiej, artystycznej oraz wypowiedzi akademickich przewidują przepisy OchrDanychU[19]. Z oczywistych przyczyn nie znajdują one zastosowania do korzystających z nadzoru wizyjnego podmiotów prowadzących działalność leczniczą i w związku z tym nie zostały omówione.

3. Prawo dostępu do danych

Kolejnym uprawnieniem podmiotu danych, o szczególnie istotnym znaczeniu z punktu widzenia osób monitorowanych, jest zagwarantowane treścią art. 15 RODO prawo dostępu do danych (rozumiane jako prawo dostępu do danych *sensu largo*). Skorzystanie z tego uprawnienia nie zostało obwarowane żadnymi szczególnymi warunkami, przysługuje więc ono każdej osobie, której dane dotyczą, w relacji z każdym podmiotem zobowiązanym do stosowania RODO. Przyjęty przez prawodawcę europejskiego model prawa dostępu do danych jest, zarówno pod względem przedmiotowym, jak i podmiotowym, bardzo szeroki. Bez wpływu na jego zakres pozostaje to, jakiej kategorii danych dotyczy przetwarzanie, w jakim celu oraz w oparciu o jaką przesłankę legalizacyjną się ono odbywa. Osoba fizyczna nie musi wykazywać ani uprawdopodabniać istnienia interesu faktycznego czy prawnego w uzyskaniu dostępu do dotyczących jej danych. Wystarczy jedynie jej **uzasadnione przypuszczenie**, że administrator przetwarza jej dane osobowe, np. przechowując nagrania z monitoringu, na których utrwalono jej wizerunek, a wskazane uprawnienie **pozwala na jego weryfikację**.

Faktyczna **realizacja prawa dostępu do danych** odbywa się w istocie **w dwóch etapach**. I tak w pierwszym z nich na administratorze spoczywa **obowiązek udzielenia podmiotowi danych informacji, czy ten przetwarza jego dane osobowe**. W drugim, stwier-

[18] Potwierdził to Prezes UODO w decyzji ZSPR.421.3.2018 z 15.3.2018 r., na mocy której po raz pierwszy w Polsce na podmiot zobowiązany do stosowania RODO nałożono administracyjną karę pieniężną. Zob. też wyr. WSA w Warszawie z 11.12.2019 r., II SA/WA 1030/19, Legalis.

[19] Więcej na temat zastosowania tych przesłanek zob. np. *M. Żmijewski*, (w:) Ustawa o ochronie danych osobowych. Komentarz, red. *D. Lubasz*, Warszawa 2019, s. 24–33 oraz *M. Gawroński*, (w:) Ustawa o ochronie danych osobowych. Komentarz, red. *D. Lubasz*, Warszawa 2019, s. 33–44.

dzenie faktu przetwarzania danych przez administratora otwiera podmiotowi danych drogę do równoległej realizacji kolejnych, powiązanych ze sobą uprawnień tj.:

1) **prawa do uzyskania informacji** dotyczących przetwarzania,
2) **prawa dostępu** do zgromadzonych danych,
3) **prawa do uzyskania kopii** danych.

Osoba objęta wideonadzorem, zgłaszając żądanie dostępowe, może wskazać, z którego z powyższych uprawnień chce skorzystać, tzn. czy jest zainteresowana realizacją jednego z nich, wybranych dwóch czy wszystkich łącznie. Jeśli z treści wniosku nie wynika żadne ograniczenie w tym przedmiocie, zespół uprawnień, o których mowa w art. 15 RODO, powinien zostać zrealizowany przez administratora w pełnym możliwym zakresie.

Odnosząc się do prawa do uzyskania informacji dotyczących przetwarzania jako składowej prawa dostępu do danych, należy zauważyć, że katalog tych informacji uzyskiwany przez podmiot danych choć rozbudowany, to jednak nie jest tożsamy z zakresem informacji udostępnianych w ramach realizacji obowiązku informacyjnego na podstawie art. 13 ust. 1 i 2 RODO, tj. w przypadku pierwotnego gromadzenia danych. Różnice w tym zakresie ilustruje tabela poniżej.

Tabela 2. Zakres informacji przekazywanych na podstawie art. 15 ust. 1 RODO i art. 13. ust. 1 i 2 RODO – porównanie

Informacje przekazywane podmiotowi danych w ramach realizacji	
prawa dostępu do danych, o którym mowa w art. 15 ust. 1 RODO	obowiązku informacyjnego, o którym mowa w art. 13 ust. 1 i 2 RODO
–	Tożsamość administratora i dane kontaktowe
–	Tożsamość i dane kontaktowe przedstawiciela administratora – gdy ma to zastosowanie
–	Dane kontaktowe inspektora ochrony danych – gdy ma to zastosowanie
Cel przetwarzania	Cel przetwarzania oraz podstawa prawna przetwarzania
Kategorie odnośnych danych osobowych	–
Informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione (w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych – a jeśli dochodzi do takiego transferu, o odpowiednich zabezpieczeniach związanych z przekazaniem, o których mowa w art. 46 RODO)	Informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją, a gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz informacje o sposobach uzyskania kopii zabezpieczeń lub o miejscu ich udostępnienia
W miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu	Okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu

Informacje przekazywane podmiotowi danych w ramach realizacji	
prawa dostępu do danych, o którym mowa w art. 15 ust. 1 RODO	**obowiązku informacyjnego, o którym mowa w art. 13 ust. 1 i 2 RODO**
Informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania	Informacje o prawie do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych
	Informacje o prawie do cofnięcia zgody w dowolnym momencie, bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem – jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO
Informacje o prawie wniesienia skargi do organu nadzorczego	Informacje o prawie wniesienia skargi do organu nadzorczego
–	Informacje, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych
Jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle	–
Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą	Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą

Źródło: opracowanie własne.

Jednym z praktycznych problemów związanych z realizacją prawa osób monitorowanych do uzyskania dostępu do danych może być **należyta weryfikacja tożsamości wnioskodawcy**. Z jednej strony, właściwą identyfikację osoby zgłaszającej żądanie dostępowe należy oceniać jako obowiązek administratora, który powinien być spełniony przy wykorzystaniu wszelkich rozsądnych środków (motyw 63 RODO), z drugiej zaś to podmiot danych zainteresowany realizacją przysługujących mu praw będzie dostarczał administratorowi takich informacji, które w efekcie doprowadzą do wykazania jego tożsamości.

Pamiętać przy tym należy, że zgodnie z art. 11 ust. 1 RODO, jeżeli cele, w których administrator przetwarza dane osobowe, nie wymagają lub już nie wymagają zidentyfikowania przez niego osoby, której dane dotyczą, administrator nie ma obowiązku zachowania, uzyskania ani przetworzenia dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą, wyłącznie po to, by zastosować się do RODO. Jeśli w takim przypadku administrator może wykazać, że nie jest w stanie zidentyfikować podmiotu danych, np. jedynie na podstawie przesłanego w celu potwierdzenia tożsamości zdjęcia,

powinien w miarę możliwości poinformować o tym podmiot danych. W takich przypadkach dochodzi do wyłączenia stosowania art. 15–20 RODO, chyba że dana osoba fizyczna w celu wykonania przysługujących jej praw, o których mowa we wskazanych przepisach, w tym także prawa dostępu do danych, dostarczy administratorowi dodatkowych informacji pozwalających na jej zidentyfikowanie. Stąd też administrator może skutecznie argumentować, że stosując monitoring na dużym obszarze, w stosunku do wielu osób przy wykorzystaniu rozbudowanej sieci kamer, a nie dysponując systemem rozpoznawania twarzy, nie jest w stanie wychwycić tych przypadków, w których doszło do utrwalenia wizerunku osoby zwracającej się z żądaniem dostępowym. Z drugiej strony, na taką identyfikację w większości przypadków pozwoli podanie dodatkowo przez osobę objętą wideonadzorem np. przybliżonej godziny wejścia na obszar monitorowany i określenie terenu, po którym się poruszała (np. parter szpitala, okolice przychodni XYZ). Stąd też, jak wskazuje EROD, administrator powinien wcześniej powiadomić podmiot danych, jakie informacje pozwolą mu na spełnienie zgłoszonego żądania[20]. Ponadto, organ ten w swoich wytycznych dotyczących przetwarzania danych przy wykorzystaniu urządzeń wideo stwierdził, że nawet jeśli administrator będzie potrafił wykazać, że nie jest w stanie zidentyfikować osoby, której dane dotyczą, to powinien przekazać jej informacje dotyczące stosowania przez niego wideomonitoringu (np. o tym, jaki dokładnie obszar został objęty monitoringiem), które pozwolą jej na pełne zrozumienie, jakie jej dane były przetwarzane[21].

Uprawnienia, o których mowa w art. 15 RODO, **realizowane są w wyniku złożenia wniosku** przez osobę, której dane dotyczą, przy czym pojęcie wniosku należy tu utożsamiać z żądaniem czy prośbą, nie zaś z pismem w rozumieniu rozdziału VIII KPA. Zwrócenie się do administratora z żądaniem realizacji prawa dostępu do danych **nie jest obwarowane żadnymi szczególnymi wymogami formalnymi** – może ono zostać zgłoszone wszelkimi, dostępnymi kanałami komunikacji z danym administratorem, np. pisemnie, telefonicznie czy za pośrednictwem poczty elektronicznej. Zgodnie z art. 12 ust. 2 oraz motywem 59 RODO administrator powinien przewidzieć **procedury ułatwiające podmiotowi danych wykonywanie wszystkich przysługujących mu praw**, w tym także prawa dostępu do danych. Jedną z form składania żądań, które administrator powinien zapewnić, jest forma elektroniczna (motyw 59 RODO), co nie oznacza, że może być to jedyny dostępny kanał komunikacji z administratorem.

Przykład

Za niedopuszczalne uznać należy wprowadzenie przez placówkę medyczną regulaminu, który za skutecznie wniesione uznaje tylko żądanie dostępu do nagrań z monitoringu złożone przy wykorzystaniu specjalnego formularza elektronicznego dostępnego na stronie internetowej.

Z drugiej strony, wniesienie żądania w formie elektronicznej wiąże administratora co do sposobu realizacji prawa dostępu do danych w ten sposób, że w miarę możliwości informacje i kopia danych także powinny wnioskodawcy zostać przekazane elektronicznie, chyba że wskaże on inną formę (art. 15 ust. 3 RODO). Projektując możliwe formy składa-

20 Europejska Rada Ochrony Danych, Wytyczne dotyczące przetwarzania danych osobowych z wykorzystaniem urządzeń wideo..., s. 22.
21 Tamże.

nia żądań dostępowych i sposób ich rozpatrywania, **administrator powinien uwzględnić**:

1) potrzebę udokumentowania, **jakiej treści i kiedy żądanie dostępowe zostało wniesione**,
2) konieczność należytej **weryfikacji tożsamości podmiotu** wnoszącego żądanie,
3) wymóg, aby **komunikacja z podmiotem danych** odbywała się m.in. w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie (art. 12 ust. 1 RODO).

Administrator musi udzielić podmiotowi danych informacji o działaniach, które podjął w związku z żądaniem dostępu do danych **bez zbędnej zwłoki, jednak nie później niż w terminie miesiąca** od otrzymania wniosku. Termin ten może zostać przedłużony maksymalnie o kolejne 2 miesiące z uwagi na jego skomplikowany charakter lub liczbę żądań, przy czym o przedłużeniu terminu należy zawsze poinformować podmiot danych, podając jednocześnie przyczyny opóźnienia. Zasada ta obowiązuje zresztą wszystkich administratorów, do których podmioty danych zwróciły się z żądaniem realizacji przysługujących im praw.

Za **okoliczności będące podstawą przedłużenia terminu** w przypadku złożenia wniosku dostępowego uznać można żądanie dostępu do nagrań z monitoringu obejmujących znaczny przedział czasowy lub jedynie przybliżony przedział czasowy, duży obszar monitorowany, fakt że na nagraniach znajdują się inne osoby, co pociąga za sobą konieczność zanonimizowania ich wizerunku, a jeśli jest to niemożliwe, udostępnienia jedynie fragmentów nagrań. Szczególnie problematyczne może być uczynienie zadość żądaniu przekazania kopii danych tych osób, których wizerunek jest utrwalany za pomocą kamer monitoringu szczególnie często (np. pracowników placówki medycznej). Należy wówczas pamiętać, że zgodnie z motywem 63 RODO administrator przetwarzający duże ilości informacji o osobie, której dane dotyczą, ma **możliwość zażądania, przed podaniem informacji, by osoba ta sprecyzowała objęte żądaniem informacje lub czynności przetwarzania**. Jeśli z kolei osoba objęta wideonadzorem, w ramach prawa dostępu do danych żąda równoległej realizacji kilku przysługujących jej uprawnień, należy je realizować niezależnie od siebie, np. niezwłocznie udzielić informacji dotyczących przetwarzania, a następnie, po wydłużeniu terminu do zrealizowania tego obowiązku, przekazać kopię danych.

Nie należy również zapominać, że zgodnie z art. 15 ust. 4 RODO prawo do uzyskania kopii danych nie może niekorzystnie wpływać na prawa i wolności innych. Dotyczy to również osób, których wizerunek utrwalono na nagraniach wraz z wizerunkiem osoby zgłaszającej administratorowi żądanie wydania nagrania z monitoringu. Jak słusznie podkreśla EROD, w takich przypadkach administrator powinien sięgnąć po narzędzia pozwalające na skuteczną anonimizację danych tych osób, nie zaś wykorzystywać ten fakt jako pretekst do odmowy podmiotom danych realizacji przysługujących im na mocy art. 15 RODO praw [22].

[22] Tamże, s. 22–23.

4. Pozostałe prawa korekcyjne i zakazowe

Wśród innych uprawnień, które mogą być realizowane przez osobę monitorowaną w relacji z administratorem wykorzystującym monitoring wizyjny jako narzędzie przetwarzania danych, wskazać należy przede wszystkim dobrze znane już pod rządami dyrektywy 95/46/WE **prawo do usunięcia danych** (art. 12 lit. b dyrektywy 95/46/WE). Treścią tego uprawnienia jest żądanie niezwłocznego usunięcia danych dotyczących podmiotu danych ze wszystkich zasobów administratora, które jest skuteczne w przypadku wystąpienia choćby jednej z przesłanek, o których mowa w art. 17 ust. 1 RODO. W przypadku stosowania monitoringu wizyjnego przez placówki medyczne, wśród okoliczności stanowiących podstawę do żądania przez osobę monitorowaną niezwłocznego usunięcia nagrań, na których utrwalono jej wizerunek czy inne cechy ją identyfikujące z katalogu wskazanego w RODO, należy przede wszystkim przywołać przypadki, w których:

1) dane nie są już niezbędne do celów, w których zostały zebrane lub były w inny sposób przetwarzane,
2) dane muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator,
3) dane były przetwarzane niezgodnie z prawem,
4) podmiot danych wniósł sprzeciw wobec przetwarzania[23].

Okoliczności, w których dane nie są już niezbędne do realizacji celów, w których zostały zebrane lub w inny sposób przetwarzane oraz dane muszą zostać usunięte w celu wywiązania się przez administratora z obowiązku prawnego należy w przypadku administratorów stosujących monitoring wizyjny wiązać przede wszystkim z okresami retencji gromadzonych danych. Podstawowym terminem przechowywania nagrań z monitoringu dla tych placówek medycznych jest okres do 3 miesięcy od dnia ich sporządzenia – odnosi się on zarówno do nagrań z miejsc ogólnodostępnych, jak i nagrań z monitoringu stosowanego wobec pracowników. Po jego upływie osoby monitorowane mogą więc skutecznie domagać się usunięcia ich danych, chyba że np. nagrania z ich wizerunkiem mają stanowić dowód w postępowaniu o zniszczenie mienia pracodawcy[24]. Zastosowanie w odniesieniu do osób monitorowanych może również znaleźć przesłanka przetwarzania ich danych niezgodnie z prawem, np. w przypadku sporządzania nagrań z kamer monitoringu zamontowanych w szatni, mimo że dopuszczalność ich stosowania nie wynika z przepisów szczególnych (por. art. 23a ust. 1 pkt 2 DziałLeczU) albo przechowywania nagrań z monitoringu mimo upływu okresu ich retencji, gdy nie zachodzi inna podstawa do przetwarzania danych. Podkreślić należy, że **stwierdzenia braku zgodności z prawem przetwarzania danych może i powinien w takich przypadkach dokonać sam administrator, nie czekając w tym przedmiocie na rozstrzygnięcie Prezesa UODO**.

---

[23] Chodzi o sprzeciw zgłoszony przez podmiot danych na mocy art. 21 ust. 1 RODO wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub wniesiony na mocy art. 21 ust. 2 RODO.

[24] Art. 22^2 KP przewiduje, że w przypadku, w którym nagrania obrazu stanowią dowód w postępowaniu prowadzonym na podstawie prawa lub pracodawca dowiedział się, że mogą one stanowić dowód w takim postępowaniu, okres ich retencji ulega przedłużeniu do czasu prawomocnego zakończenia postępowania.

Kolejną z okoliczności stanowiących podstawę do skutecznego żądania usunięcia danych jest wcześniejsze wniesienie przez podmiot danych **sprzeciwu wobec ich dalszego przetwarzania** – z przyczyn związanych z jej szczególną sytuacją przy jednoczesnym braku nadrzędnych, prawnie uzasadnionych podstaw do dokonywania takich operacji na danych osobowych, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń. Prawo do sprzeciwu będzie przysługiwało osobom monitorowanym w przypadku, w którym oparte jest ono na przesłance prawnie uzasadnionego interesu, tj. art. 6 ust. 1 lit. f RODO. Dotyczy więc ono przypadków legalnego przetwarzania danych zwykłych, którego administrator ma zaprzestać z uwagi na szczególną sytuację podmiotu danych. Wniesienie sprzeciwu może nastąpić w każdym czasie po przekroczeniu granicy obszaru monitorowanego – zarówno w trakcie, jak i po jego opuszczeniu[25], a powinno wywołać skutek w postaci konieczności wykonania przez administratora ponownego testu równowagi – ważenia interesu administratora leżącego u podstaw przetwarzania oraz okoliczności, na które powołuje się osoba, której dane dotyczą[26]. Dopiero wykazanie przez administratora, że istnieją ważne prawnie uzasadnione podstawy do przetwarzania danych, które mają charakter nadrzędny wobec interesów, praw i wolności osoby monitorowanej lub nagrania z monitoringu służą jako materiał do ustalenia, dochodzenia lub obrony roszczeń, pozwala na dalsze przetwarzanie danych, np. w postaci ich posiadania. W innych przypadkach sprzeciw podmiotu danych będzie skuteczny i otworzy drogę do żądania usunięcia dotyczących jej danych na podstawie art. 17 ust. 1 lit. c RODO. Do czasu stwierdzenia przez administratora, czy występujące po jego stronie prawnie uzasadnione podstawy przetwarzania są nadrzędne wobec podstaw sprzeciwu osoby monitorowanej, podmiot danych może skorzystać z prawa do żądania ograniczenia przetwarzania danych (art. 18 ust. 1 lit. d RODO).

Ważne

Usunięcie danych w przypadku ich przetwarzania przy pomocy monitoringu wizyjnego może polegać zarówno na trwałym usunięciu fragmentu lub całości nagrania, zniszczeniu nośnika, na którym był utrwalony, ale również np. na anonimizacji wizerunku podmiotu danych poprzez taką obróbkę obrazu, aby jego odtworzenie było niemożliwe[27].

Wskazując na przesłanki pozwalające osobie monitorowanej na skuteczne żądanie usunięcia dotyczących jej nagrań, nie sposób nie odnieść się również do akcesoryjnego w stosunku do niego **prawa do bycia zapomnianym**. Uprawnienie to, wyinterpretowane przez TSUE w poprzednim stanie prawnym z art. 12 lit. b dyrektywy 95/46/WE (zob. wyr. TSUE z 13.5.2014 r., C-131/12, *Google Spain SL v. Agencia de Proteccion de Da-*

25 Europejska Rada Ochrony Danych, Wytyczne dotyczące przetwarzania danych osobowych z wykorzystaniem urządzeń wideo..., s. 24.

26 Nie wystarczy w tym przypadku odwołać się jedynie do analizy dokonanej w związku z oparciem przetwarzania na art. 6 ust. 1 lit. f RODO – tak: Grupa Robocza Art. 29, (w:) Grupa Robocza Art. 29, Wytyczne w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE, przyjęte w dniu 3.10.2017 r., ostatnio zmienione i przyjęte w dniu 6.2.2018 r., WP 251, s. 21.

27 Za usunięcie danych przetwarzanych przy wykorzystaniu nagrań wideo należy również uznać ich nieodwracalną anonimizację, np. poprzez rozmazanie obrazu, na co zwróciła uwagę EROD w swoich wytycznych – zob. Wytyczne dotyczące przetwarzania danych osobowych z wykorzystaniem urządzeń wideo..., s. 24.

tos (AEPD) i Mario Costeja González, Legalis; wyr. TSUE z 9.3.2017 r., C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, Legalis)[28] ukonstytuowano i rozwinięto treścią art. 17 ust. 2 RODO. Generalnie prawo do bycia zapomnianym będzie mogło być zrealizowane przez podmioty danych jedynie w stosunku do danych upublicznionych przez administratora i jedynie w przypadkach, w których:

1) spełniona została co najmniej jedna z przesłanek pozwalających na skorzystanie z prawa do usunięcia danych, a jednocześnie
2) nie zachodzi żadna z przesłanek negatywnych wskazanych w art. 17 ust. 3 RODO.

Wówczas obowiązkiem administratora jest nie tylko usunięcie upublicznionych przez niego danych, np. poprzez usunięcie fragmentu nagrania z monitoringu z własnej strony internetowej, ale również przy uwzględnieniu dostępnej technologii i kosztów realizacji – podjęcie tzw. rozsądnych działań, w tym środków technicznych, aby poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

Prawo do usunięcia danych, podobnie jak prawo do bycia zapomnianym, **nie ma charakteru bezwzględnego** i zostaje ono wyłączone w przypadkach, w których przetwarzanie jest niezbędne m.in. do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator oraz do ustalenia, dochodzenia lub obrony roszczeń[29]. Dlatego też osoba monitorowana nie może skutecznie żądać od administratora usunięcia z jego zasobów nagrań, co do których nie upłynął jeszcze wymagany prawem okres retencji, np. trwający minimum 12, a maksimum 13 miesięcy termin przechowywania nagrań z monitoringu stosowanego w pomieszczeniach przeznaczonych do izolacji, o których mowa w art. 18e ust. 1 ZdrPsychU.

Wśród innych uprawnień, które RODO przyznaje podmiotom danych, w kontekście przetwarzania danych przy wykorzystaniu nagrań z monitoringu wizyjnego, należy odnieść się również do **prawa do ograniczenia przetwarzania**. Sprowadza się ono do żądania, aby administrator zaprzestał dokonywania jakichkolwiek innych operacji na danych osobowych poza ich przechowywaniem (art. 18 ust. 2 RODO). W przypadku skutecznego skorzystania przez podmiot danych z tego uprawnienia pozostałe działania na danych wymagają albo zgody tego podmiotu, albo są dopuszczalne jedynie w przypadkach wskazanych w art. 18 ust. 2 RODO, tj. w celu ustalenia, dochodzenia lub obrony roszczeń, lub ochrony praw innej osoby fizycznej lub prawnej, lub ze względu na ważne względy inte-

[28] Zob. też *M. Czerniawski*, Glosa do wyroku TS z 13.5.2014 r., C-131/12, Lex/el. 2014.

[29] Jak stanowi art. 17 ust. 3 RODO, prawo do usunięcia danych oraz prawo do bycia zapomnianym nie znajdą zastosowania do przypadków, w których przetwarzanie jest niezbędne: 1) do korzystania z prawa do wolności wypowiedzi i informacji; 2) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi; 3) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h oraz i, a także art. 9 ust. 3 RODO; 4) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub 5) do ustalenia, dochodzenia lub obrony roszczeń.

resu publicznego Unii lub państwa członkowskiego. Prawodawca europejski zagwarantował możliwość skorzystania z prawa do ograniczenia przetwarzania m.in. w przypadku, w którym administrator nie potrzebuje już danych do celów przetwarzania, ale są one potrzebne podmiotowi danych do ustalenia, dochodzenia lub obrony roszczeń (art. 18 ust. 1 lit. c RODO). Jest to istotna przesłanka z punktu widzenia osób, wobec których stosowany jest nadzór wizyjny, gdyż **pozwala ona na zobowiązanie administratora do przechowywania nagrania z monitoringu mimo upływającego okresu retencji**. Osoba monitorowana może również w praktyce powołać się na inną okoliczność uzasadniającą ograniczenie przetwarzania, tj. sytuację, w której przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych, żądając w zamian ograniczenia ich wykorzystywania (art. 18 ust. 1 lit. b RODO).

Podmiot danych, który przypuszcza, że zastosowany wobec niego monitoring był bezprawny, może, żądając od administratora ograniczenia przetwarzania, doprowadzić do faktycznego zabezpieczenia nagrań z tego monitoringu, do czasu złożenia skargi do organu nadzorczego. Usunięcie nagrań zawierających dane objęte ograniczeniem przetwarzania wymaga zgody osoby, której dane przetwarzano w sposób niezgodny z prawem, a przed ewentualnym uchyleniem takiego ograniczenia administrator ma obowiązek poinformować ją o takim planowanym działaniu (art. 18 ust. 3 RODO). Żądanie ograniczenia przetwarzania przysługuje również podmiotowi danych w przypadku wniesienia sprzeciwu wobec przetwarzania na podstawie art. 21 ust. 1 RODO – do czasu ustalenia przez administratora, do którego sprzeciw wniesiono, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą (art. 18 ust. 1 lit. d RODO). Jednocześnie pamiętać należy, że prawo do ograniczenia przetwarzania nie powinno być wykorzystywane przez osoby monitorowane do utrudniania administratorowi dochodzenia roszczeń przysługujących mu od osób, których dane dotyczą, dlatego nawet mimo wystąpienia okoliczności uzasadniających ograniczenie przetwarzania, **administrator może je przetwarzać w celu ustalenia, dochodzenia lub obrony roszczeń** (art. 18 ust. 2 RODO).

Istotną, zarówno z punktu widzenia stosujących monitoring administratorów, jak i monitorowanych podmiotów danych, konsekwencją skutecznego skorzystania przez osobę, której dane dotyczą, z prawa do usunięcia danych czy ograniczenia przetwarzania **jest obowiązek powiadomienia o tym fakcie każdego odbiorcy**, któremu te dane ujawniono (art. 19 RODO)[30]. Spoczywa on na każdym administratorze, chyba że takie powiadomienie jest niemożliwe lub będzie wymagać niewspółmiernego wysiłku. Co więcej, administrator będzie musiał poinformować podmiot danych o takich odbiorcach, jeśli tylko osoba ta zgłosi takie żądanie.

Z uwagi na specyfikę monitoringu wizyjnego jako narzędzia przetwarzania danych **nie wszystkie prawa podmiotów danych będą mogły być realizowane przez osoby objęte wideonadzorem.** Z takim ograniczeniem podmioty danych spotkają się w przypadku chęci skorzystania z uprawnienia do żądania niezwłocznego sprostowania nieprawidłowych danych oraz żądania uzupełnienia danych niekompletnych, z uwzględnieniem celów przetwarzania (art. 16 RODO). Nagrania z monitoringu stanowią utrwalenie

[30] Obowiązek taki powstaje również w przypadku sprostowania danych.

pewnego wycinka rzeczywistości, zatem z założenia są one zgodne z tą rzeczywistością. Jedynie w przypadkach szczególnych, w których wizerunek podmiotu danych na nagraniu z monitoringu jest przetwarzany w połączeniu z innymi jego danymi, może wchodzić w grę sprostowanie tych danych, np. gdy algorytm identyfikacji twarzy mylnie przypisał ją do innego nazwiska czy funkcji. Sytuacje takie nie dotyczą jednak większości administratorów, a biorąc pod uwagę cel przetwarzania danych w przypadku stosowania nadzoru wizyjnego przez placówki medyczne, możliwość ich wystąpienia w praktyce ocenić należy jako znikomą. Podobnie, biorąc pod uwagę przesłanki legalizujące takie przetwarzanie, osobom monitorowanym nie będzie przysługiwało prawo do przenoszenia danych[31]. Mając z kolei na względzie specyfikę takiego przetwarzania, prawo do niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, o którym mowa w art. 22 RODO, ocenić należy, w odniesieniu do monitorowanych pacjentów, pracowników i osób trzecich, jako bezprzedmiotowe.

Podstawa prawna:

- art. 5 ust. 1 lit. a, art. 6 ust. 1 lit. f, art. 11 ust. 1 i 2, art. 12–22, 27 ust. 1, art. 83 ust. 5 lit. b, motyw 59 i 63 RODO,
- art. 12 lit. b dyrektywy 95/46/WE,
- art. 22^2 KP,
- art. 23a DziałLeczU,
- art. 29 WymDziałLeczR,
- art. 18e ZdrPsychU,
- art. 102 ust. 1 i 2 OchrDanychU.

[31] Zob. art. 20 RODO.