Wytyczne 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo

Wersja 2.0

przyjęta 29 stycznia 2020 r.

Historia wersji

Wersja 2.1	26 lutego 2021 r.	Poprawa istotnego błędu
Wersja 2.0	29 stycznia 2020 r.	Przyjęcie wytycznych po konsultacjach publicznych
Wersja 1.0	10 lipca 2019 r.	Przyjęcie wytycznych do konsultacji publicznych

Spis treści

Europejska Rada Ochrony Danych

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanego dalej „RODO"),

uwzględniając Porozumienie EOG, a w szczególności jego załącznik XI i protokół 37, w brzmieniu zmienionym decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[1],

uwzględniając art. 12 i 22 swojego regulaminu wewnętrznego,

PRZYJMUJE NINIEJSZE WYTYCZNE

1 WPROWADZENIE

1. Częste korzystanie z urządzeń wideo wpływa na zachowanie obywateli. Znaczący poziom wdrożenia takich narzędzi w wielu sferach życia osoby wywierać będzie na nią dodatkową presję celem zapobieżenia wykryciu tego, co może być postrzegane jako anomalie. Technologie te mogą *de facto* ograniczać możliwości anonimowego przemieszczania się oraz anonimowego korzystania z usług i generalnie ograniczać możliwość pozostania niezauważonym. Skutki dla ochrony danych są ogromne.

2. Podczas gdy osoby mogą nie mieć nic przeciwko monitoringowi wizyjnemu zainstalowanemu na przykład w określonym celu związanym z bezpieczeństwem, należy ustanowić gwarancje celem uniknięcia niewłaściwego wykorzystywania danych w zupełnie innych i – dla osób, których dane dotyczą – nieoczekiwanych celach (np. w celach marketingowych, monitorowania wydajności pracownika itd.). Ponadto obecnie wdraża się wiele narzędzi służących wykorzystaniu utrwalonych wizerunków i przekształceniu tradycyjnych kamer w inteligentne kamery. Ilość danych generowanych przez nagrania wideo, w połączeniu z tymi narzędziami i technikami, zwiększa ryzyko ich wtórnego wykorzystania (bez względu na to, czy jest ono związane z celem pierwotnie przypisanym systemowi) lub nawet ryzyko związane z niewłaściwym wykorzystaniem danych. Mając do czynienia z monitoringiem wizyjnym, zawsze należy starannie rozważyć ogólne zasady określone w RODO (art. 5).

3. Systemy monitoringu wizyjnego pod wieloma względami zmieniają sposób, w jaki profesjonaliści z sektorów prywatnego i publicznego wchodzą w interakcje w miejscach prywatnych i publicznych w celu zwiększenia bezpieczeństwa, uzyskania analizy publiczności, dostarczenia spersonalizowanych reklam itd. Monitoring wizyjny stał się wysoce skuteczny za sprawą wdrażania na coraz większą skalę inteligentnej analizy obrazu. Techniki te mogą być bardziej (np. złożone technologie biometryczne) lub mniej inwazyjne (np. proste algorytmy liczące). Pozostawanie anonimowym oraz zachowanie prywatności staje się co do zasady coraz trudniejsze. Kwestie związane z ochroną danych podniesione

[1] Odniesienia do „państw członkowskich" w niniejszej opinii należy rozumieć jako odniesienia do „państw członkowskich EOG".

w różnych sytuacjach mogą się różnić, podobnie analiza prawna przy korzystaniu z którejkolwiek z tych technologii.

4. Oprócz kwestii prywatności istnieją również ryzyka związane z ewentualnym nieprawidłowym działaniem tych urządzeń oraz uprzedzeń, które mogą wywoływać. Badacze zauważają, że oprogramowanie wykorzystywane do identyfikacji, rozpoznawania i analizy twarzy działa inaczej w zależności od wieku, płci i pochodzenia etnicznego osoby identyfikowanej. Algorytmy działają w oparciu o zróżnicowane dane demograficzne, w związku z tym stronniczość rozpoznawania twarzy stwarza ryzyko pogłębienia uprzedzeń w społeczeństwie. Dlatego też administratorzy danych muszą również zapewnić, aby przetwarzanie danych biometrycznych, pochodzących z monitoringu wizyjnego, podlegało regularnej ocenie jego istotności i wystarczalności zastosowanych gwarancji.

5. Monitoring wizyjny nie jest domyślnie niezbędny, gdy istnieją inne środki umożliwiające osiągnięcie założonego celu. W przeciwnym razie ryzykujemy zmianę w zakresie norm kulturowych, prowadzącą do zaakceptowania braku prywatności jako warunku startowego.

6. Niniejsze wytyczne mają na celu zapewnienie wskazówek dotyczących stosowania przepisów RODO w związku z przetwarzaniem danych osobowych przez urządzenia wideo. Przedstawione przykłady nie mają charakteru wyczerpującego, ogólny sposób rozumowania można zastosować w odniesieniu do wszystkich potencjalnych obszarów stosowania.

2 ZAKRES STOSOWANIA[2]

2.1 Dane osobowe

7. Systematyczny zautomatyzowany monitoring konkretnego obszaru za pomocą środków optycznych lub audiowizualnych, głównie w celu ochrony mienia lub ochrony życia i zdrowia osoby, stał się znaczącym zjawiskiem naszych czasów. Działanie to wiąże się z gromadzeniem i zatrzymywaniem informacji związanych z obrazem lub audiowizualnych, dotyczących wszystkich osób wchodzących na obszar monitorowany, które można zidentyfikować na podstawie ich wyglądu lub innych cech szczególnych. Szczegóły te często umożliwiają ustalenie tożsamości tych osób. Monitoring umożliwia również dalsze przetwarzanie danych osobowych dotyczących obecności osób i ich zachowania na danym obszarze. Potencjalne ryzyko niewłaściwego wykorzystania danych zwiększa się wraz z wielkością monitorowanego obszaru, jak również z liczbą osób na nim przebywających. Fakt ten znajduje odzwierciedlenie w art. 35 ust. 3 lit. c) RODO, który wymaga przeprowadzenia oceny skutków dla ochrony danych w przypadku systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie, jak również art. 37 ust. 1 lit. b), który wymaga od podmiotów przetwarzających wyznaczenia inspektora ochrony danych w przypadku, gdy operacje przetwarzania, ze względu na swój charakter, wiążą się z regularnym i systematycznym monitorowaniem osób, których dane dotyczą.

8. Rozporządzenie nie ma jednak zastosowania do przetwarzania danych, które nie odnoszą się do konkretnej osoby, np. jeżeli bezpośrednio lub pośrednio nie można zidentyfikować osoby.

> Przykład: RODO nie ma zastosowania do atrap kamer (tj. kamer, które nie funkcjonują jako kamery i w związku z tym nie przetwarzają żadnych danych osobowych). *W niektórych państwach członkowskich kwestia ta może jednak podlegać innym przepisom.*
>
> Przykład: Nagrania wykonane na dużych wysokościach wchodzą w zakres stosowania RODO wyłącznie wtedy, jeżeli w danych okolicznościach przetwarzane dane mogą być powiązane z konkretną osobą.
>
> Przykład: Samochód jest wyposażony w kamerę wideo, która ma pomóc kierowcy w parkowaniu. RODO nie ma zastosowania, jeżeli kamera jest skonstruowana lub dostosowana w taki sposób, że nie gromadzi żadnych informacji dotyczących osoby fizycznej (takich jak numery tablic rejestracyjnych lub informacje, które mogłyby służyć identyfikacji przechodniów).

9.

2.2 Stosowanie dyrektywy 2016/680

10. W zakres stosowania dyrektywy (UE) 2016/680 wchodzi zwłaszcza przetwarzanie danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

[2] Europejska Rada Ochrony Danych (EROD) zauważa, że – jeżeli zezwalają na to przepisy RODO – w przepisach krajowych mogą mieć zastosowanie szczególne wymogi.

2.3 Wyjątek domowy i osobisty

11. Zgodnie z art. 2 ust. 2 lit. c) w zakres stosowania RODO nie wchodzi przetwarzanie danych osobowych przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze [3].

12. W kontekście monitoringu wizyjnego należy przyjąć wąską interpretację niniejszego przepisu – tzw. wyjątku domowego i osobistego. Zatem, jak uznał Trybunał Sprawiedliwości Unii Europejskiej, tzw. „wyjątek domowy i osobisty" powinien być „interpretowany jako obejmujący wyłącznie działania wchodzące w zakres życia prywatnego lub rodzinnego jednostki, co w sposób oczywisty nie ma miejsca w przypadku przetwarzania danych osobowych polegającego na ich opublikowaniu w internecie w taki sposób, że staną się one dostępne dla nieograniczonej liczby osób"[4]. Ponadto jeżeli system monitoringu wizyjnego, w zakresie, w jakim obejmuje on ciągłe nagrywanie i przechowywanie danych osobowych i rozciąga się „choćby częściowo na przestrzeń publiczną i tym samym jest skierowany poza sferę prywatną osoby dokonującej w ten sposób przetwarzania danych, o tyle nie powinien on być rozumiany jako czynność o czysto »osobistym lub domowym charakterze« w rozumieniu art. 3 ust. 2 tiret drugie dyrektywy 95/46"[5].

13. Jeżeli chodzi o urządzenia wideo działające na prywatnej posiadłości danej osoby, mogą one być objęte wyjątkiem domowym i osobistym. Będzie to uzależnione od kilku czynników, które należy w pełni rozważyć, aby wyciągnąć odpowiednie wnioski. Poza wyżej wymienionymi elementami wskazanymi w orzeczeniach TSUE, użytkownik domowego monitoringu wizyjnego musi rozważyć, czy łączą go jakiekolwiek relacje osobiste z osobą, której dane dotyczą, czy skala i częstotliwość monitoringu wskazują na jakąkolwiek działalność zawodową z jego strony, a także potencjalny niekorzystny wpływ monitoringu na osoby, których dane dotyczą. Obecność któregokolwiek z wyżej wymienionych elementów niekoniecznie sugeruje, że przetwarzanie wykracza poza zakres wyjątku domowego i osobistego: aby to stwierdzić, należy dokonać całościowej oceny.

> Przykład: Turysta nagrywa materiał video zarówno telefonem komórkowym, jak i kamerą, aby udokumentować swoje wakacje. Pokazuje nagrania przyjaciołom i rodzinie, lecz nie udostępnia ich nieograniczonej liczbie osób. Taka sytuacja byłaby objęta wyjątkiem domowym i osobistym.
>
> Przykład: Kobieta uprawiająca kolarstwo górskie chce nagrać swój zjazd kamerą sportową. Jeździ ona w odludnym miejscu i zamierza wykorzystać te nagrania wyłącznie do osobistej rozrywki. Taka sytuacja byłaby objęta wyjątkiem domowym i osobistym, nawet jeżeli dane osobowe byłyby w pewnym zakresie przetwarzane.
>
> Przykład: Ktoś monitoruje i nagrywa swój własny ogród. Nieruchomość jest ogrodzona i tylko sam administrator oraz jego rodzina wchodzą do ogrodu regularnie. Taka sytuacja byłaby objęta wyjątkiem domowym i osobistym, pod warunkiem że monitoring wizyjny nie rozciąga się nawet częściowo na przestrzeń publiczną lub sąsiednią nieruchomość.

14.

[3] Zobacz również motyw 18.

[4] Trybunał Sprawiedliwości Unii Europejskiej, wyrok w sprawie C–101/01, Bodil Lindqvist, z dnia 6 listopada 2003 r., pkt 47.

[5] Trybunał Sprawiedliwości Unii Europejskiej, wyrok w sprawie C–212/13, František Ryneš przeciwko Úřad pro ochranu osobních údajů, z dnia 11 grudnia 2014 r., pkt 33.

3 ZGODNOŚĆ PRZETWARZANIA Z PRAWEM

15. Przed rozpoczęciem korzystania z monitoringu wizyjnego należy szczegółowo określić cele przetwarzania (art. 5 ust. 1 lit. b) RODO). Monitoring wizyjny może służyć różnym celom, np. wspieraniu ochrony mienia i majątku, wspieraniu ochrony życia i integralności cielesnej osób, gromadzeniu dowodów przy roszczeniach cywilnych[6]. Te cele monitorowania należy udokumentować na piśmie (art. 5 ust. 2 RODO) i określić w odniesieniu do każdej kamery używanej do monitorowania wizyjnego. Kamery wykorzystywane w tym samym celu przez jednego administratora danych mogą zostać objęte wspólną dokumentacją. Ponadto należy poinformować osoby, których dane dotyczą, o celu lub celach przetwarzania zgodnie z art. 13 (*zob. Rozdział 7, Przejrzystość i obowiązki informacyjne*). Monitoring wizyjny oparty wyłącznie na podstawie, jaką jest cel „bezpieczeństwa" lub „własnego bezpieczeństwa" nie jest pojęciem wystarczająco konkretnym (art. 5 ust. 1 lit. b)). Ponadto jest on sprzeczny z zasadą stanowiącą, że dane osobowe są przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (zob. art. 5 ust. 1 lit. a)).

16. Co do zasady każda podstawa prawna określona w art. 6 ust. 1 może stanowić podstawę prawną przetwarzania danych pochodzących z monitoringu wizyjnego. Na przykład art. 6 ust. 1 lit. c) ma zastosowanie w przypadku, gdy przepisy krajowe przewidują obowiązek prowadzenia monitoringu wizyjnego[7]. Jednakże w praktyce najprawdopodobniej zostaną zastosowane następujące przepisy:

- art. 6 ust. 1 lit. f) (prawnie uzasadniony interes),
- art. 6 ust. 1 lit. e) (niezbędność wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej).

W wyjątkowych przypadkach art. 6 ust. 1 lit. a) (zgoda) może służyć administratorowi jako podstawa prawna przetwarzania.

3.1 Prawnie uzasadniony interes, art. 6 ust. 1 lit. f)

17. Ocena prawna art. 6 ust. 1 lit. f) powinna opierać się na następujących kryteriach zgodnie z motywem 47.

3.1.1 Istnienie prawnie uzasadnionych interesów

18. Monitoring wizyjny jest zgodny z prawem, o ile jest niezbędny do osiągnięcia celu prawnie uzasadnionego interesu administratora danych lub strony trzeciej, chyba że interesy te są podrzędne wobec interesów osoby, której dane dotyczą, lub podstawowych praw i wolności (art. 6 ust. 1 lit. f)). Prawnie uzasadnione interesy administratora lub strony trzeciej mogą być interesami prawnymi[8], gospodarczymi lub niematerialnymi[9]. Administrator danych powinien jednak wziąć pod uwagę, że jeżeli osoba, której dane dotyczą, wnosi sprzeciw wobec monitorowania zgodnie z art. 21, administrator może prowadzić monitoring wizyjny wobec tej osoby, której dane dotyczą, wyłącznie

[6] Przepisy dotyczące gromadzenia dowodów przy roszczeniach cywilnych różnią się w poszczególnych państwach członkowskich.

[7] Niniejsze wytyczne nie stanowią analizy ani szczegółowego przeglądu przepisów krajowych, które mogą różnić się w poszczególnych państwach członkowskich.

[8] Trybunał Sprawiedliwości Unii Europejskiej, wyrok w sprawie C–13/16, *sprawa Rigas satiksme*, z dnia 4 maja 2017 r.

[9] Zob. opinię WP217 Grupy Roboczej Art. 29.

jeżeli stanowi on *ważny* prawnie uzasadniony interes, który jest nadrzędny w stosunku do interesów, praw i wolności osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia i obrony roszczeń.

19. Biorąc pod uwagę realną i niebezpieczną sytuację, cel ochrony nieruchomości przed włamaniem, kradzieżą lub aktami wandalizmu może stanowić prawnie uzasadniony interes dla monitoringu wizyjnego.

20. Prawnie uzasadniony interes musi mieć wymiar realny i stanowić kwestię bieżącą (tj. nie może być fikcyjny lub spekulatywny)[10]. Przed rozpoczęciem monitoringu musi zaistnieć sytuacja rzeczywistego zagrożenia – np. szkody lub poważne incydenty, które miały miejsce w przeszłości. Zgodnie z zasadą rozliczalności, administratorzy powinni dokumentować istotne incydenty (datę, rodzaj, straty finansowe) oraz związane z nimi zarzuty. Takie udokumentowane incydenty mogą stanowić mocne dowody na istnienie prawnie uzasadnionego interesu. Istnienie prawnie uzasadnionego interesu, jak również konieczność monitorowania, powinny podlegać ponownej ocenie w regularnych odstępach czasu (np. raz na rok, w zależności od okoliczności).

> Przykład: Właściciel sklepu chce otworzyć nowy sklep i zainstalować system monitoringu wizyjnego, aby nie dopuścić do aktów wandalizmu. Przedstawiając odpowiednie statystyki może on wykazać, że w najbliższym sąsiedztwie istnieje duże prawdopodobieństwo wystąpienia aktów wandalizmu. Doświadczenia właścicieli sąsiednich sklepów również mogą okazać się przydatne. Administrator, o którym mowa, nie musi ponieść jakichkolwiek szkód. O ile szkody wyrządzone w sąsiedztwie wskazują na wystąpienie jakiegokolwiek niebezpieczeństwa, mogą wskazywać na istnienie prawnie uzasadnionego interesu. Przedstawienie krajowych lub ogólnych statystyk dotyczących przestępczości, bez przeprowadzenia analizy danego obszaru lub zagrożeń dla tego konkretnego sklepu, nie jest jednak wystarczające.

21.

22. Sytuacje stwarzające bezpośrednie zagrożenie mogą stanowić prawnie uzasadniony interes, np. banki lub sklepy zajmujące się sprzedażą cennych towarów (np. biżuterii) lub obszary, które znane są jako typowe miejsca przestępstw przeciwko mieniu (np. stacje paliw).

23. RODO wyraźnie stanowi, że organy publiczne nie mogą przetwarzać danych w oparciu o prawnie uzasadniony interes, dopóki wykonują swoje zadania, art. 6 ust. 1 zdanie 2.

3.1.2 Niezbędność przetwarzania

24. Dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych"), zob. art. 5 ust. 1 lit. c). Przed zainstalowaniem systemu monitoringu wizyjnego administrator powinien zawsze krytycznie ocenić czy środek ten, po pierwsze jest odpowiedni do osiągnięcia pożądanego celu, a po drugie odpowiedni i niezbędny do jego celów. Środki polegające na zastosowaniu monitoringu wizyjnego należy wybierać wyłącznie w przypadku, gdy cel przetwarzania nie mógł zostać osiągnięty w sposób racjonalny za pomocą innych środków, które są mniej inwazyjne w stosunku do podstawowych praw i wolności osoby, której dane dotyczą.

25. Biorąc pod uwagę sytuację, w której administrator chce zapobiec przestępstwom przeciwko mieniu, zamiast instalowania systemu monitoringu wizyjnego administrator mógłby również zastosować alternatywne środki bezpieczeństwa, takie jak ogrodzenie nieruchomości, patrole ochrony, korzystanie

[10] Zob. WP217, Grupa Robocza Art. 29, s. 24 i nn.
Zob. również wyrok TSUE w sprawie C–708/18, s. 44.

z usług strażników, zapewnienie lepszego oświetlenia, zamontowanie zamków, zainstalowanie zabezpieczeń w oknach i drzwiach czy nałożenie powłok lub folii przeciwko graffiti. Środki te mogą być równie skuteczne w zakresie zapobiegania włamaniu, kradzieży i aktom wandalizmu, co systemy monitoringu wizyjnego. Administrator musi ocenić w każdym przypadku z osobna, czy takie środki mogą stanowić racjonalne rozwiązanie.

26. Przed uruchomieniem systemu kamer administrator ma obowiązek ocenić, gdzie i kiedy zastosowanie środków monitoringu wizyjnego jest bezwzględnie konieczne. Zazwyczaj system monitoringu, który działa w porze nocnej, a także poza normalnymi godzinami pracy, sprosta potrzebom administratora w zakresie zapobieżenia ewentualnym zagrożeniom, na które narażona jest jego własność.

27. Ogólnie rzecz biorąc konieczność korzystania z monitoringu wizyjnego w celu ochrony nieruchomości administratorów kończy się na ich granicach.[11] Niemniej istnieją przypadki, w których monitorowanie nieruchomości nie jest wystarczające do zapewnienia skutecznej ochrony. W niektórych indywidualnych przypadkach konieczne może okazać się rozszerzenie zakresu monitoringu wizyjnego, aby objął swoim zasięgiem bezpośrednie otoczenie nieruchomości. W tym kontekście administrator powinien wziąć pod uwagę środki fizyczne i techniczne, na przykład blokowanie obserwacji nieistotnych obszarów lub ich zamazywanie.

> Przykład: Właściciel księgarni chce ją uchronić przed aktami wandalizmu. Co do zasady kamery powinny nagrywać jedynie to, co dzieje się na terenie samych obiektów, ponieważ do tego celu nie jest potrzebne oglądanie sąsiednich nieruchomości lub miejsc dostępnych publicznie, znajdujących się w sąsiedztwie księgarni.

28.

29. Pytania dotyczące niezbędności przetwarzania pojawiają się również w odniesieniu do sposobu przechowywania materiału dowodowego. W niektórych przypadkach niezbędne może być zastosowanie rozwiązań typu „czarnych skrzynek", w przypadku których nagranie jest automatycznie usuwane po upływie określonego okresu przechowywania i dostępne wyłącznie w przypadku wystąpienia incydentu. W innych sytuacjach rejestrowanie materiału wideo może w ogóle nie być konieczne, a bardziej odpowiednim rozwiązaniem byłoby wykorzystanie monitorowania w czasie rzeczywistym. Decyzja między wyborem rozwiązania typu „czarnych skrzynek" a monitoringiem w czasie rzeczywistym powinna być uzależniona od założonego celu. Na przykład jeżeli celem monitoringu wizyjnego jest zabezpieczenie materiału dowodowego, posługiwanie się podglądem w czasie rzeczywistym zazwyczaj nie jest odpowiednie. Monitoring w czasie rzeczywistym może być czasem bardziej inwazyjny niż przechowywanie i automatyczne usuwanie nagrań po upływie określonego terminu (np. jeżeli ktoś nieustannie spogląda na monitor, może to być podejście o wiele bardziej inwazyjne niż w przypadku braku jakiegokolwiek monitora i przechowywania nagrań bezpośrednio w „czarnej skrzynce"). W tym kontekście należy uwzględnić zasadę minimalizacji danych (art. 5 ust. 1 lit. c). Należy również pamiętać, że zamiast korzystania z monitoringu wizyjnego administrator może skorzystać z usług personelu ochrony, który jest w stanie natychmiast zareagować i zainterweniować.

3.1.3 Wyważenie interesów

30. Zakładając, że monitoring wizyjny jest niezbędny do zapewnienia ochrony prawnie uzasadnionych interesów administratora, system monitoringu wizyjnego może zostać wprowadzony do użytku wyłącznie w przypadku, gdy wobec prawnie uzasadnionych interesów administratora lub strony

[11] Taka sytuacja również może podlegać przepisom krajowym w niektórych państwach członkowskich.

trzeciej (np. ochrona mienia lub integralności cielesnej) nadrzędnego charakteru nie mają interesy lub podstawowe prawa i wolności osób, których dane dotyczą. Administrator musi uwzględnić 1) w jakim stopniu monitoring wpływa na interesy, podstawowe prawa i wolności osób fizycznych i 2) czy powoduje on naruszenia lub wywołuje negatywne skutki dla praw osób, których dane dotyczą. Wyważanie interesów ma faktycznie charakter obowiązkowy. Z jednej strony należy ocenić i z rozwagą wyważyć podstawowe prawa i wolności, a z drugiej strony prawnie uzasadnione interesy administratora.

Przykład: Prywatna firma parkingowa odnotowała powtarzające się incydenty związane z okradaniem zaparkowanych samochodów. Parking stanowi otwartą przestrzeń i jest łatwo dostępny dla wszystkich, teren ten jest jednak wyraźnie oznaczony znakami i zaporami drogowymi blokującymi przejazd. Firma parkingowa ma prawnie uzasadniony interes (zapobieganie kradzieżom w samochodach klientów) w monitorowaniu obszaru w godzinach, w których jest najbardziej narażona na wystąpienie takich incydentów. Osoby, których dane dotyczą, są monitorowane w określonym czasie, nie przebywają na tym terenie w celach rekreacyjnych, a zapobieganie kradzieżom leży również w ich interesie. Prawnie uzasadniony interes administratora ma w tym przypadku charakter nadrzędny w stosunku do interesu osób, których dane dotyczą, polegający na braku ich monitorowania.

Przykład: Właściciel restauracji postanawia zamontować kamery wideo w toaletach, aby kontrolować stan czystości pomieszczeń sanitarnych. W tym przypadku prawa osób, których dane dotyczą, mają zdecydowanie nadrzędny charakter wobec interesu administratora, a zatem w tym miejscu nie można zamontować kamer.

31.

3.1.3.1 Podejmowanie decyzji w każdym przypadku z osobna

32. W związku z tym, że zgodnie z rozporządzeniem wyważanie interesów ma charakter obowiązkowy, decyzję należy podjąć indywidualnie w każdym przypadku (zob. art. 6 ust. 1 lit. f)). Odnoszenie się do sytuacji abstrakcyjnych lub porównywanie podobnych przypadków jest niewystarczające. Administrator musi ocenić ryzyka związane z naruszeniem praw osób, których dane dotyczą; w tym przypadku decydującym kryterium jest intensywność ingerencji w prawa i wolności osób.

33. Stopień intensywności można określić m.in. w oparciu o rodzaj zgromadzonych informacji (treść informacji), zakres (gęstość informacji, zasięg przestrzenny i geograficzny), liczbę zainteresowanych osób, których dane dotyczą, jako konkretną liczbę lub jako odsetek właściwej populacji, daną sytuację, rzeczywiste interesy grupy osób, których dane dotyczą, środki alternatywne, jak również o charakter i zakres oceny danych.

34. Istotnymi czynnikami równoważącymi mogą być wielkość obszaru objętego monitoringiem oraz liczba osób, których dane dotyczą, objętych monitoringiem. Korzystanie z monitoringu wizyjnego w odludnym miejscu (np. w celu obserwowania zwierząt wolno żyjących lub ochrony infrastruktury krytycznej, takiej jak antena radiowa będąca własnością prywatną) należy oceniać w inny sposób niż monitoring wizyjny wykorzystywany w strefie pieszej lub centrum handlowym.

Przykład: W przypadku zamontowania kamery samochodowej (np. dla celów zgromadzenia dowodów w razie wypadku) należy upewnić się, że kamera ta nie nagrywa w sposób ciągły ruchu drogowego, jak również osób znajdujących się na poboczu. W przeciwnym razie interes posiadania nagrań wideo jako dowodów w razie ewentualnego wypadku drogowego nie może usprawiedliwiać poważnej ingerencji w prawa osób, których dane dotyczą[11].

35.

3.1.3.2 Rozsądne oczekiwania osób, których dane dotyczą

36. Zgodnie z motywem 47 stwierdzenie istnienia prawnie uzasadnionego interesu wymaga przeprowadzenia dokładnej oceny. Należy tu uwzględnić rozsądne oczekiwania osób, których dane dotyczą, podczas i w kontekście przetwarzania ich danych osobowych. Jeżeli chodzi o systematyczne monitorowanie, związek między osobą, której dane dotyczą, a administratorem może być zróżnicowany i wpływać na to, jakie ewentualne rozsądne oczekiwania może mieć osoba, której dane dotyczą. Wykładnia pojęcia „rozsądnych oczekiwań" nie powinna opierać się jedynie na subiektywnych oczekiwaniach. Decydującym kryterium powinno być raczej to, czy obiektywna strona trzecia mogłaby zasadnie oczekiwać i stwierdzić, że została objęta monitoringiem w tej konkretnej sytuacji.

37. Na przykład, w większości przypadków, pracownik nie oczekuje, że będzie monitorowany w swoim miejscu pracy przez pracodawcę[12]. Ponadto nie należy oczekiwać, że monitoring będzie funkcjonował w czyimś prywatnym ogrodzie, w mieszkaniu lub w gabinetach lekarskich i zabiegowych. Z tego samego względu nie jest rozsądne oczekiwanie monitoringu w pomieszczeniach sanitarnych lub saunach – monitorowanie takich pomieszczeń stanowi poważną ingerencję w prawa osób, których dane dotyczą. Rozsądne oczekiwania osób, których dane dotyczą, zakładają że monitoring wizyjny nie zostanie zamontowany w wyżej wymienionych miejscach. Z drugiej strony klient banku może oczekiwać, że jest monitorowany na terenie banku lub w pobliżu bankomatu.

38. Osoby, których dane dotyczą, mogą również oczekiwać, że nie będą monitorowane w miejscach dostępnych publicznie, zwłaszcza jeżeli miejsca te zwykle służą regeneracji, rekonwalescencji i wypoczynkowi, a także w miejscach, w których osoby przebywają lub komunikują się ze sobą, takich jak przestrzenie z wyznaczonymi miejscami do siedzenia, stoliki w restauracjach, parki, kina i centra fitness. W tym przypadku interesy lub prawa i wolności osób, których dane dotyczą, często będą miały nadrzędny charakter w stosunku do prawnie uzasadnionych interesów administratora.

> Przykład: Osoby, których dane dotyczą, nie oczekują, że będą monitorowane w toaletach. Monitoring wizyjny używany na przykład w celu zapobieżenia wypadkom nie jest proporcjonalnym środkiem.

39.

40. Znaki informujące osoby, których dane dotyczą, o monitoringu wizyjnym nie są istotne przy określaniu obiektywnych oczekiwań osób, których dane dotyczą. Oznacza to, że np. właściciel sklepu nie może powoływać się na obiektywnie żywione, rozsądne oczekiwania klienta dotyczące monitorowania tylko dlatego, że znak informuje daną osobę o obecności monitoringu już przy wejściu do sklepu.

[12] Zob. także: Grupa Robocza Art. 29, Opinia 2/2017 na temat przetwarzania danych w miejscu pracy, WP 249, przyjęta w dniu 8 czerwca 2017 r.

3.2 Niezbędność wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 6 ust. 1 lit. e))

41. Dane osobowe mogą być przetwarzane za pośrednictwem monitoringu wizyjnego zgodnie z art. 6 ust. 1 lit. e) jeżeli jest to niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej[13]. Może się okazać, że wykonywanie władzy publicznej nie zezwala na takie przetwarzanie, lecz inne podstawy prawne, takie jak „zdrowie i bezpieczeństwo" dla ochrony odwiedzających i pracowników mogą zapewniać podstawę dla ograniczonego zakresu przetwarzania, przy jednoczesnym uwzględnieniu obowiązków wynikających z RODO i praw osób, których dane dotyczą.

42. Państwa członkowskie mogą utrzymać w mocy lub wprowadzać w życie szczegółowe przepisy krajowe w celu dostosowania zakresu stosowania przepisów RODO dla monitoringu wizyjnego poprzez bardziej precyzyjne określenie szczegółowych wymogów przetwarzania, o ile są one zgodne z zasadami określonymi w RODO (np. ograniczenie przechowywania, proporcjonalność).

3.3 Zgoda, art. 6 ust. 1 lit. a)

43. Zgoda musi zostać wyrażona dobrowolnie, być konkretna, świadoma i jednoznaczna, jak określono w wytycznych dotyczących zgody[14].

44. Jeżeli chodzi o systematyczne monitorowanie, zgoda osoby, której dane dotyczą, może służyć w wyjątkowych przypadkach jako podstawa prawna, jedynie jeżeli jest zgodna z art. 7 (zob. motyw 43). Cechą charakterystyczną monitoringu jest to, że technologia ta monitoruje nieznaną liczbę osób w tym samym czasie. Administratorowi będzie trudno udowodnić, że osoba, której dane dotyczą, wyraziła zgodę przed przetwarzaniem swoich danych osobowych (art. 7 ust. 1). Zakładając, że osoba, której dane dotyczą, wycofa zgodę, administratorowi trudno będzie udowodnić, że jej dane osobowe nie są już przetwarzane (art. 7 ust. 3).

> Przykład: Sportowcy mogą domagać się uruchomienia monitoringu w trakcie ćwiczeń indywidualnych w celu późniejszej analizy swojej techniki i wyników. Z drugiej strony, w przypadku gdy klub sportowy podejmie inicjatywę w zakresie monitorowania całego zespołu w tym samym celu, w większości przypadków zgoda ta nie będzie ważna, gdyż poszczególni sportowcy mogą czuć się zmuszeni do wyrażenia zgody, aby ich odmowa nie wpłynęła negatywnie na kolegów z drużyny.

45.

46. W przypadku gdy administrator zamierza polegać na udzielonej zgodzie, musi zapewnić, aby każda osoba, której dane dotyczą, wchodząca na obszar objęty monitoringiem wizyjnym, wyraziła zgodę na objęcie monitorowaniem. Zgoda ta musi spełniać warunki określone w art. 7. Wejście na oznaczony obszar objęty monitoringiem (np. ludzie zachęcani są do przejścia przez specjalny korytarz lub bramkę, aby wejść na teren objęty monitoringiem) nie stanowi oświadczenia lub jednoznacznej,

[13] Podstawa przetwarzania, o którym mowa powyżej, musi być określona w prawie Unii lub państwa członkowskiego i „musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi" (art. 6 ust. 3).

[14] Grupa Robocza Art. 29 (GR Art. 29) „Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679" (WP 259 rev. 01) – zatwierdzone przez EROD.

potwierdzającej czynności, niezbędnych do wyrażenia zgody, chyba że spełnia kryteria z art. 4 i 7, opisane w wytycznych dotyczących zgody[15].

47. Z uwagi na brak równowagi sił między pracodawcami i pracownikami, w większości przypadków pracodawcy nie powinni opierać się na zgodzie przy przetwarzaniu danych osobowych, ponieważ jest mało prawdopodobnym, że zostanie ona udzielona dobrowolnie. W tym kontekście należy wziąć pod uwagę wytyczne dotyczące zgody.

48. W prawie państwa członkowskiego lub w porozumieniach zbiorowych, w tym zakładowych porozumieniach z przedstawicielami pracowników, mogą być przewidziane przepisy szczegółowe o przetwarzaniu danych osobowych pracowników w związku z zatrudnieniem (zob. art. 88).

[15] Grupa Robocza Art. 29 (GR Art. 29) „Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679" (WP 259) – zatwierdzone przez EROD – które należy wziąć pod uwagę.

4 UJAWNIENIE NAGRAŃ WIDEO STRONOM TRZECIM

49. Co do zasady do ujawniania nagrań wideo stronom trzecim stosuje się przepisy RODO.

4.1 Ujawnienie nagrań wideo stronom trzecim – zarys

50. Pojęcie „ujawniania" zdefiniowano w art. 4 ust. 2 jako przesłanie (np. komunikacja indywidualna), rozpowszechnianie (np. publikowanie w internecie) lub innego rodzaju udostępnianie. Pojęcie „strony trzeciej" zdefiniowano w art. 4 ust. 10. W przypadku ujawnienia danych państwom trzecim lub organizacjom międzynarodowym zastosowanie mają również przepisy szczególne określone w art. 44 i nn.

51. Wszelkie ujawnienie danych osobowych stanowi odrębny rodzaj przetwarzania danych osobowych, dla którego administrator potrzebuje podstawy prawnej określonej w art. 6.

> Przykład: Administrator, który zamierza umieścić nagranie w internecie, musi oprzeć się na podstawie prawnej dla tego przetwarzania, np. uzyskując zgodę osoby, której dane dotyczą, zgodnie z art. 6 ust. 1 lit. a).

52.

53. Nagrania wideo mogą zostać przesłane stronom trzecim w celu innym niż cel, w którym dane osobowe zostały zebrane, na podstawie przepisów art. 6 ust. 4.

> Przykład: Aby umożliwić rozstrzyganie kwestii odszkodowań za ewentualne powstałe szkody, zamontowano monitoring wizyjny rogatki (na parkingu). Powstaje szkoda i nagranie zostaje przesłane prawnikowi w celu zainicjowania sprawy. W tym przypadku cel nagrywania jest taki sam jak cel przesyłania.
>
> Przykład: Aby umożliwić rozstrzyganie kwestii odszkodowań za ewentualne powstałe szkody zamontowano monitoring wizyjny rogatki (na parkingu). Nagranie zostaje opublikowane w internecie wyłącznie w celach rozrywkowych. W tym przypadku cel uległ zmianie i nie jest zgodny z celem pierwotnym. Ponadto określenie podstawy prawnej dla tego przetwarzania (opublikowanie) stanowiłoby problem.

54.

55. Strona trzecia będąca odbiorcą będzie musiała sama przeprowadzić analizę prawną, w szczególności określając na podstawie art. 6 podstawę prawną dla swoich operacji przetwarzania danych (np. przy otrzymywaniu materiałów).

4.2 Ujawnienie nagrań wideo organom ścigania

56. Ujawnienie nagrań wideo organom ścigania jest również niezależnym procesem, wymagającym od administratora odrębnego uzasadnienia.

57. Zgodnie z art. 6 ust. 1 lit. c) przetwarzanie jest zgodne z prawem, jeżeli jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. Mimo iż obowiązujące prawo dotyczące policji pozostaje pod wyłączną kontrolą państw członkowskich, w każdym państwie członkowskim istnieją zapewne ogólne zasady regulujące przekazywanie materiału dowodowego organom ścigania. Operacje przetwarzania danych przez administratora polegające na przekazywaniu danych są uregulowane przez RODO. W przypadku gdy przepisy krajowe nakładają na administratora obowiązek współpracy z organami ścigania (np. prowadzenia postępowania przygotowawczego), podstawą prawną przekazywania danych jest obowiązek prawny, o którym mowa w art. 6 ust. 1 lit. c).

58. W takim przypadku ograniczenie celu, o którym mowa w art. 6 ust. 4, zazwyczaj nie jest problematyczne, ponieważ ujawnienie wyraźnie odwołuje się do prawa państwa członkowskiego. W związku z tym uwzględnianie szczególnych wymogów w odniesieniu do zmiany celu w kontekście lit. a)–e) nie jest niezbędne.

59. Przykład: Właściciel sklepu nagrywa materiał wideo obejmujący wejście do niego. Na nagraniu widać osobę, która kradnie portfel innej osobie. Policja prosi administratora o przekazanie nagrań na potrzeby przeprowadzenia postępowania przygotowawczego. W takim przypadku właściciel sklepu wykorzystałby podstawę prawną, o której mowa w art. 6 ust. 1 lit. c), (obowiązek prawny), czytaną łącznie z odpowiednimi przepisami krajowymi dotyczącymi przetwarzania w postaci przekazywania danych.

60. Przykład: Ze względów bezpieczeństwa w sklepie zamontowano kamerę. Właściciel sklepu uważa, że zarejestrował coś podejrzanego, więc postanawia przesłać nagranie policji (bez posiadania informacji o jakimkolwiek prowadzonym postępowaniu przygotowawczym). W tym przypadku właściciel sklepu musi ocenić, czy zostały spełnione warunki, o których mowa (w większości przypadków) w art. 6 ust. 1 lit. f). Jest tak zazwyczaj, gdy właściciel sklepu ma uzasadnione podejrzenie, że doszło do popełnienia przestępstwa.

61. Przetwarzanie danych osobowych przez same organy ścigania nie podlega pod przepisy RODO (zob. art. 2 ust. 2 lit. d)), lecz pod dyrektywę 2016/680.

5 PRZETWARZANIE SZCZEGÓLNYCH KATEGORII DANYCH

62. Systemy monitoringu wizyjnego gromadzą zazwyczaj ogromne ilości danych osobowych, które mogą ujawniać dane o charakterze wysoce osobistym, a nawet szczególne kategorie danych. Pozornie nieistotne dane, zgromadzone za pośrednictwem nagrań wideo, mogą być wykorzystywane do wywnioskowania innych informacji do osiągniecia innego celu (np. mapowania nawyków osób). Monitoring wizyjny nie zawsze jest jednak uznawany za przetwarzający szczególne kategorie danych osobowych.

> Przykład: Nagranie wideo przedstawiające osobę, której dane dotyczą, w okularach lub na wózku inwalidzkim, nie jest samo w sobie uważane za szczególną kategorię danych osobowych.

63.

64. Jeżeli nagranie wideo jest jednak przetwarzane w celu wydedukowania szczególnych kategorii danych, zastosowanie ma art. 9.

> Przykład: Opinie polityczne można na przykład wywnioskować ze zdjęć, na których znajdują się możliwe do zidentyfikowania osoby, których dane dotyczą, uczestniczące w danym wydarzeniu, biorące udział w strajku itd. Taka sytuacja byłaby objęta zakresem stosowania art. 9.
>
> Przykład: Szpital, który zainstalował kamerę wideo w celu monitorowania stanu zdrowia pacjenta, zostałby uznany za przetwarzający szczególne kategorie danych osobowych (art. 9).

65.

66. Co do zasady, w przypadku każdego instalowania systemu monitoringu wizyjnego, należy starannie rozważyć zasadę minimalizacji danych. W związku z tym nawet w przypadkach, w których art. 9 ust. 1 nie ma zastosowania, administrator danych powinien zawsze próbować minimalizować ryzyko utrwalenia nagrania ujawniającego inne dane wrażliwe (wykraczające poza zakres art. 9), niezależnie od celu.

> Przykład: Monitoring wizyjny utrwalający wizerunek kościoła sam w sobie nie jest objęty zakresem art. 9. Administrator musi jednak dokonać wyjątkowo starannej oceny zgodnie z art. 6 ust. 1 lit. f), uwzględniając charakter danych oraz ryzyko utrwalenia innych wrażliwych danych (wykraczających poza zakres art. 9) przy ocenie interesów osób, których dane dotyczą.

67.

68. Jeżeli system monitoringu wizyjnego jest wykorzystywany do przetwarzania szczególnych kategorii danych, administrator danych musi określić zarówno wyjątek dla przetwarzania szczególnych kategorii danych zgodnie z art. 9 (tj. odstępstwo od ogólnej zasady stanowiącej, że nie należy przetwarzać szczególnych kategorii danych) oraz podstawę prawną zgodnie z art. 6.

69. Na przykład art. 9 ust. 2 lit. c) („[...] przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej [...]") mógłby – teoretyczne i w wyjątkowych przypadkach – zostać wykorzystany, administrator danych musiałby jednak uzasadnić to bezwzględną niezbędnością zabezpieczenia żywotnych interesów osoby i udowodnić, że ta "[…] osoba, której dane dotyczą, *jest fizycznie lub prawnie niezdolna do wyrażenia zgody*". Ponadto administrator danych nie będzie mógł korzystać z systemu w żadnym innym celu.

70. Należy zauważyć, że nie każde odstępstwo wymienione w art. 9 może być użyte jako uzasadnienie przetwarzania szczególnych kategorii danych za pośrednictwem monitoringu wizyjnego. Konkretniej: administratorzy danych przetwarzający te dane w kontekście monitoringu wizyjnego nie mogą opierać się na art. 9 ust. 2 lit. e), który zezwala na przetwarzanie odnoszące się do danych osobowych w sposób oczywisty upublicznionych przez osobę, której dotyczą. Sam fakt wejścia w zasięg kamery nie oznacza, że osoba, której dane dotyczą, zamierza upublicznić szczególne kategorie danych, które jej dotyczą.

71. Ponadto przetwarzanie szczególnych kategorii danych wymaga wzmożonej i nieustannej czujności w odniesieniu do pewnych obowiązków; na przykład wysokiego poziomu bezpieczeństwa i oceny skutków dla ochrony danych, gdy jest to niezbędne.

> Przykład: Pracodawca nie może wykorzystywać nagrań z monitoringu wizyjnego przedstawiających demonstrację w celu zidentyfikowania strajkujących.

72.

5.1 Względy ogólne dotyczące przetwarzania danych biometrycznych

73. Wykorzystywanie danych biometrycznych, a zwłaszcza technologii rozpoznawania twarzy, wiąże się ze zwiększonymi ryzykami dla praw osób, których dane dotyczą. Kluczowe jest, by korzystanie z takich technologii odbywało się z należytym uwzględnieniem zasad zgodności z prawem, konieczności, proporcjonalności i minimalizacji danych, jak określono w RODO. Podczas gdy używanie takich technologii może być postrzegane jako szczególnie skuteczne, administratorzy powinni jednak najpierw ocenić ich wpływ na podstawowe prawa i wolności oraz rozważyć zastosowanie mniej inwazyjnych środków do osiągnięcia prawnie uzasadnionego celu przetwarzania.

74. Aby dane zostały zakwalifikowane jako dane biometryczne, zgodnie z definicją RODO, przetwarzanie surowych danych, takich jak cechy fizyczne, fizjologiczne lub behawioralne osoby fizycznej, musi zakładać pomiar tych cech. Z uwagi na to, iż dane biometryczne są wynikiem takich pomiarów, art. 4 ust. 14 RODO stanowi, że dane te „[...] wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby [...]". Nagranie wideo danej osoby nie może zostać jednak uznane samo w sobie jako zawierające dane biometryczne zgodnie z art. 9, jeżeli nie zostały one specjalnie przetworzone technicznie w celu identyfikacji tej osoby[16].

75. Aby przetwarzanie zostało uznane za przetwarzanie szczególnych kategorii danych osobowych (art. 9), dane biometryczne muszą być przetwarzane „w celu jednoznacznego zidentyfikowania osoby fizycznej".

76. Podsumowując, w świetle art. 4 ust. 14 i art. 9 należy uwzględnić trzy kryteria:

- **Charakter danych:** dane dotyczące cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej,
- **Środki i sposób przetwarzania**: dane, które „wynikają ze specjalnego przetwarzania technicznego",

[16] Motyw 51 RODO wspiera tę analizę stanowiąc, że „[...] Przetwarzanie fotografii nie powinno zawsze stanowić przetwarzania szczególnych kategorii danych osobowych, gdyż fotografie są objęte definicją »danych biometrycznych« tylko w przypadkach, gdy są przetwarzane specjalnymi metodami technicznymi, umożliwiającymi jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości. […]".

- **Cel przetwarzania:** dane muszą być wykorzystane w celu jednoznacznego zidentyfikowania osoby fizycznej.

77. Wykorzystywanie monitoringu wizyjnego, w tym funkcji rozpoznawania biometrycznego, zamontowanego przez podmioty prywatne dla swoich celów (np. w celach marketingowych, statystycznych lub nawet bezpieczeństwa) w większości przypadków będzie wymagało wyraźnej zgody wszystkich osób, których dane dotyczą (art. 9 ust. 2 lit. a)), jednakże zastosowanie może mieć inny odpowiedni wyjątek, o którym mowa w art. 9.

> Przykład: Aby udoskonalić swoje usługi spółka prywatna zastępuje punkty identyfikacji pasażerów na lotnisku (punkt nadania bagażu, wejście na pokład) systemami monitoringu wizyjnego, które wykorzystują techniki rozpoznawania twarzy w celu sprawdzenia tożsamości pasażerów, którzy wyrazili zgodę na poddanie się takiej procedurze. Z uwagi na to, że przetwarzanie wchodzi w zakres art. 9, pasażerowie, którzy uprzednio wyraźnie i świadomie wyrazili swoją zgodę, będą musieli się zarejestrować w automatycznym terminalu w celu stworzenia i zarejestrowania „szablonu" twarzy przypisanego do ich karty pokładowej i dowodu tożsamości. Punkty kontroli z funkcją rozpoznawania twarzy muszą być wyraźnie oddzielone, tzn. system należy zainstalować w bramce, aby szablony biometryczne osoby, która nie wyraża na to zgody, nie zostały zarejestrowane. Tylko pasażerowie, którzy uprzednio wyrazili zgodę i kontynuowali rejestrację, skorzystają z bramki wyposażonej w system biometryczny.
>
> Przykład: Administrator zarządza dostępem do swojego budynku przy wykorzystaniu metody rozpoznawania twarzy. Odwiedzający mogą korzystać z tego rodzaju dostępu po uprzednim wyraźnym i świadomym wyrażeniu zgody (zgodnie z art. 9 ust. 2 lit. a)). Niemniej, aby mieć pewność, że nie utrwalono wizerunku żadnej osoby, która uprzednio nie wyraziła na to zgody, metoda rozpoznawania twarzy powinna zostać uruchomiona przez samą osobę, której dane dotyczą, na przykład poprzez wciśnięcie przycisku. Aby zapewnić zgodność przetwarzania z prawem, administrator zawsze musi zaproponować alternatywny sposób uzyskania dostępu do budynku, bez przetwarzania biometrycznego, np. za pomocą identyfikatorów lub kluczy.

78.

79. W tego rodzaju przypadkach, gdy tworzy się szablony biometryczne, administratorzy powinni zapewnić, aby po uzyskaniu wyniku dopasowania lub niedopasowania wszystkie pośrednie szablony wykonane w tle (za wyraźną i świadomą zgodą osoby, której dane dotyczą) w celu porównania ich do tych stworzonych przez osoby, których dane dotyczą, w trakcie rejestracji, zostały niezwłocznie i w bezpieczny sposób usunięte. Szablony stworzone na potrzeby rejestracji powinny być zachowane jedynie do realizacji celu przetwarzania i nie powinny być przechowywane ani archiwizowane.

80. Jeżeli jednak celem przetwarzania jest na przykład odróżnienie jednej kategorii osób od innej, ale nie jednoznaczne zidentyfikowanie danej osoby, wówczas przetwarzanie nie wchodzi w zakres art. 9.

> Przykład: Właściciel sklepu chciałby spersonalizować reklamy w oparciu o cechy związane z płcią i wiekiem klienta utrwalone przez system monitoringu wizyjnego. W przypadku gdy system ten nie generuje szablonów biometrycznych w celu jednoznacznego zidentyfikowania osób, a zamiast tego wykrywa jedynie te cechy fizyczne, aby przypisać daną osobę do konkretnej grupy, wówczas przetwarzanie nie wchodzi w zakres art. 9 (o ile nie jest przetwarzany żaden inny rodzaj szczególnych kategorii danych).

81.

82. Art. 9 ma jednak zastosowanie w przypadku gdy administrator przechowuje dane biometryczne (zazwyczaj za pośrednictwem szablonów tworzonych w wyniku wyodrębnienia najważniejszych cech z

surowej formy danych biometrycznych (np. wymiarów twarzy ze zdjęcia)), aby jednoznacznie zidentyfikować daną osobę. Jeżeli administrator chce wykryć przypadki ponownego wejścia osoby, której dane dotyczą, na dany obszar lub wejścia na inny obszar (np. w celu dalszego wyświetlania spersonalizowanych reklam), wówczas celem będzie jednoznaczne zidentyfikowanie osoby fizycznej, co oznacza, że od samego początku procedura ta wchodziłaby w zakres art. 9. Tak mogłoby być w przypadku, gdy administrator przechowuje wygenerowane szablony w celu dalszego umieszczania spersonalizowanych reklam na różnych bilbordach w różnych miejscach w sklepie. Z uwagi na to, że system wykorzystuje cechy fizyczne do wykrywania konkretnych osób ponownie wchodzących na obszar objęty zasięgiem kamery (np. osób odwiedzających centrum handlowe) i śledzenia ich, stanowiłoby to metodę identyfikacji biometrycznej, ponieważ ma na celu rozpoznanie z wykorzystaniem specjalnego przetwarzania technicznego.

> Przykład: Właściciel sklepu zainstalował system rozpoznawania twarzy na terenie obiektu, aby dopasować swoje reklamy do potrzeb klientów. Administrator danych musi uzyskać wyraźną i świadomą zgodę wszystkich osób, których dane dotyczą, przed wykorzystaniem systemu biometrycznego i dostarczeniem spersonalizowanych reklam. System byłby niezgodny z prawem gdyby utrwalał wizerunek odwiedzających lub przechodniów, którzy nie wyrazili zgody na stworzenie ich szablonów biometrycznych, nawet jeżeli szablon ten zostałby usunięty w możliwie jak najkrótszym czasie. Takie tymczasowe szablony biometryczne rzeczywiście stanowią dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby, która może nie życzyć sobie otrzymywania spersonalizowanych reklam.

83.

84. EROD zauważa, że niektóre systemy biometryczne są instalowane w środowiskach niekontrolowanych[17], co oznacza, że system obejmuje utrwalanie w tle twarzy wszystkich osób fizycznych znajdujących się w zasięgu kamery, w tym osób, które nie wyraziły zgody na wykorzystanie urządzenia biometrycznego, a zatem na stworzenie szablonów biometrycznych. Szablony te porównuje się do tych stworzonych na potrzeby osób, których dane dotyczą, które uprzednio wyraziły zgodę w trakcie procesu rejestracji (tj. użytkowników urządzeń biometrycznych), aby administrator danych mógł stwierdzić, czy dana osoba jest użytkownikiem urządzeń biometrycznych. W tym przypadku system jest często zaprojektowany w taki sposób, by odróżnić osoby, które chce rozpoznać na podstawie bazy danych od tych, które nie zostały zarejestrowane. Z uwagi na to, że celem jest jednoznaczne zidentyfikowanie osób fizycznych, wyjątek określony w art. 9 ust. 2 RODO jest nadal potrzebny dla każdej osoby, której wizerunek został utrwalony przez kamerę.

[17] Oznacza to, że urządzenie biometryczne mieści się w ogólnodostępnej przestrzeni i może działać w przypadku każdego przechodnia, w przeciwieństwie do systemów biometrycznych w kontrolowanych środowiskach, które mogą być wykorzystywane jedynie przy udziale osoby, która wyraziła zgodę.

Przykład: Hotel korzysta z monitoringu wizyjnego w celu automatycznego powiadomienia menadżera hotelu o przybyciu ważnej osobistości (*ang. VIP*) zaraz po rozpoznaniu wizerunku takiej osoby. Osoby te uprzednio udzieliły wyraźnej zgody na wykorzystywanie funkcji rozpoznawania twarzy przed zarejestrowaniem ich wizerunku w bazie danych utworzonej w tym celu. Te systemy przetwarzania danych biometrycznych byłyby niezgodne z prawem, chyba że wszyscy pozostali goście objęci monitoringiem (w celu zidentyfikowania VIP-ów) wyraziliby zgodę na przetwarzanie zgodnie z art. 9 ust. 2 lit. a) RODO.

Przykład: Administrator instaluje system monitoringu wizyjnego z funkcją rozpoznawania twarzy przy wejściu na salę koncertową, którą zarządza. Administrator musi zapewnić wyraźnie oddzielone wejścia; jedno z systemem biometrycznym i jedno bez takiego systemu (gdzie można zamiast tego np. zeskanować bilet). Wejścia wyposażone w urządzenia biometryczne muszą zostać zbudowane i udostępnione w sposób, który uniemożliwia utrwalanie przez system szablonów biometrycznych widzów, którzy nie wyrazili na to zgody.

85.

86. Wreszcie, w przypadku gdy zgoda jest wymagana na podstawie art. 9 RODO, administrator danych nie powinien uzależniać udzielenia dostępu do swoich usług od zaakceptowania przetwarzania biometrycznego. Innymi słowy, zwłaszcza gdy przetwarzanie biometryczne wykorzystywane jest w celu uwierzytelnienia, administrator danych musi zaproponować alternatywne rozwiązanie, które nie obejmuje przetwarzania biometrycznego – bez ograniczeń lub dodatkowych kosztów dla osoby, której dane dotyczą. Takie alternatywne rozwiązanie jest również niezbędne dla osób, które nie mogą sprostać ograniczeniom urządzenia biometrycznego (niemożność rejestracji lub odczytu danych biometrycznych, trudności z korzystaniem z urządzenia ze względu na niepełnosprawność itd.), zaś w sytuacji, gdy przewiduje się, że korzystanie z urządzenia biometrycznego nie będzie możliwe (np. ze względu na nieprawidłowe działanie), należy przyjąć rozwiązanie ”rezerwowe”, aby zapewnić ciągłość zaproponowanych usług, ograniczonego jednak do działania w wyjątkowych okolicznościach. W wyjątkowych przypadkach przetwarzanie biometryczne stanowić może główną działalność w ramach usług świadczonych na podstawie umowy, np. muzeum, które organizuje wystawę, aby zaprezentować wykorzystanie urządzenia do rozpoznawania twarzy, w którym to przypadku osoby, których dane dotyczą, nie będą mogły odrzucić przetwarzania danych biometrycznych, gdyby wyraziły chęć wzięcia udziału w wystawie. W takim przypadku zgoda wymagana na podstawie art. 9 nadal jest ważna, jeżeli zostaną spełnione wymogi określone w art. 7.

5.2 Proponowane środki minimalizujące ryzyko przy przetwarzaniu danych biometrycznych

87. Zgodnie z zasadą minimalizacji danych administratorzy danych muszą zapewnić, aby dane pobrane z wizerunku cyfrowego celem stworzenia szablonu nie były nadmierne i zawierały jedynie informacje wymagane w określonym celu, unikając tym samym jakiegokolwiek ewentualnego dalszego przetwarzania. Należy wdrożyć środki w celu zapewnienia, by szablony nie mogły być przesyłane między systemami biometrycznymi.

88. W ramach identyfikacji i uwierzytelniania/weryfikacji najprawdopodobniej niezbędne będzie przechowywanie szablonu w celu jego wykorzystania w późniejszych porównaniach. Administrator danych musi wybrać najbardziej odpowiednie miejsce przechowywania danych. W środowisku kontrolowanym (odgraniczone korytarze lub punkty kontroli) szablony przechowuje się na indywidualnym urządzeniu będącym własnością użytkownika i pozostającym pod jego wyłączną kontrolą (na smartfonie lub w dowodzie tożsamości) lub – gdy są niezbędne do osiągnięcia określonych celów i w przypadku występowania obiektywnych potrzeb – przechowuje się je w scentralizowanej

bazie danych w zaszyfrowanej formie, do której klucz dostępu posiada jedynie dana osoba, w celu zapobieżenia nieuprawnionemu dostępowi do szablonu lub miejsca przechowywania. Jeżeli administrator danych nie może zapobiec posiadaniu dostępu do szablonów, musi podjąć odpowiednie kroki, aby zapewnić bezpieczeństwo przechowywanych danych. Może się to wiązać z koniecznością zaszyfrowania szablonu za pomocą algorytmu kryptograficznego.

89. W każdym przypadku administrator podejmuje wszelkie niezbędne środki ostrożności, aby zachować dostępność, integralność i poufność przetwarzanych danych. W tym celu administrator podejmuje przede wszystkim następujące środki: kategoryzuje dane w trakcie ich przesyłania i przechowywania, przechowuje szablony biometryczne i surowe dane lub dane dotyczące tożsamości w odrębnych bazach danych, szyfruje dane biometryczne, zwłaszcza szablony biometryczne i określa politykę w zakresie szyfrowania i zarządzania kluczami kryptograficznymi, wdraża środki organizacyjne i techniczne w zakresie wykrywania oszustw, przypisuje kod uwierzytelniania wiadomości do danych (np. podpis lub skrót) i zapobiega jakiemukolwiek dostępowi do danych biometrycznych z zewnątrz. Takie środki będą musiały być modyfikowane wraz z postępem technologicznym.

90. Poza tym administratorzy danych powinni usunąć surowe dane (wizerunki twarzy, sygnały mowy, sposób chodzenia itd.) i zapewnić, aby takie usunięcie było skuteczne. Jeżeli przestaje istnieć podstawa prawna przetwarzania, należy usunąć surowe dane. O ile szablony biometryczne są tworzone na podstawie takich danych, można rzeczywiście uznać, że utworzenie baz danych mogłoby stanowić równie duże, o ile nie większe, zagrożenie (ponieważ odczytanie szablonu biometrycznego nie zawsze może okazać się łatwym zadaniem bez posiadania wiedzy na temat sposobu, w jaki został on utworzony, podczas gdy surowe dane będą stanowiły elementy niezbędne do utworzenia jakiegokolwiek szablonu). W razie konieczności przechowywania takich danych przez administratora danych, należy rozważyć/zbadać metody addytywne (takie jak dodawanie znaku wodnego), które sprawiłyby, że utworzenie szablonu byłoby nieskuteczne. Administrator musi również usunąć dane i szablony biometryczne w przypadku nieuprawnionego dostępu do terminala służącego porównywaniu odczytów lub serwera przeznaczonego do przechowywania danych oraz usunąć wszystkie dane, które nie są niezbędne do dalszego przetwarzania, pod koniec cyklu życia urządzenia biometrycznego.

6 PRAWA OSOBY, KTÓREJ DANE DOTYCZĄ

91. Z uwagi na charakter przetwarzania danych przy korzystaniu z monitoringu wizyjnego, niektóre prawa osób, których dane dotyczą, przewidziane w RODO muszą zostać dodatkowo objaśnione. Niniejszy rozdział nie ma jednak charakteru wyczerpującego, wszystkie prawa przewidziane w RODO mają zastosowanie do przetwarzania danych osobowych za pośrednictwem monitoringu wizyjnego.

6.1 Prawo dostępu

92. Osoba, której dane dotyczą, ma prawo do uzyskania potwierdzenia ze strony administratora odnośnie do tego, czy jej dane są przetwarzane, czy też nie. W przypadku monitoringu wizyjnego oznacza to, że jeżeli nie przechowuje się ani nie przesyła żadnych danych po zakończeniu okresu, w którym miało miejsce monitorowanie w czasie rzeczywistym, administrator mógłby jedynie przekazać informację o tym, że nie są już przetwarzane żadne dane osobowe (oprócz ogólnych obowiązków informacyjnych, określonych w art. 13, zob. sekcja 7, Przejrzystość i obowiązki informacyjne). Jeżeli w chwili wniesienia żądania dane są jednak nadal przetwarzane (tj. jeżeli dane są przechowywane lub w sposób ciągły przetwarzane w jakikolwiek inny sposób), osoba, której dane dotyczą, powinna uzyskać dostęp i informacje zgodnie z art. 15.

93. Istnieje jednak szereg ograniczeń, które w niektórych przypadkach mogą mieć zastosowanie w związku z prawem dostępu.

- Art. 15 ust. 4 RODO: niekorzystny wpływ na prawa innych osób

94. Z uwagi na fakt, że w tej samej sekwencji monitoringu wizyjnego można zarejestrować dowolną liczbę osób, których dane dotyczą, przegląd nagrania mógłby spowodować dodatkowe przetwarzanie danych osobowych innych osób, których dane dotyczą. Jeżeli osoba, której dane dotyczą, zechce uzyskać kopię nagrań (art. 15 ust. 3) mogłoby to niekorzystnie wpłynąć na prawa i wolności innych osób, których dane dotyczą, których wizerunek został utrwalony na tym nagraniu. Aby temu zapobiec, administrator powinien zatem wziąć pod uwagę fakt, że z uwagi na inwazyjny charakter nagrań wideo administrator w niektórych przypadkach nie powinien przekazywać nagrań wideo, na których można zidentyfikować inne osoby, których dane dotyczą. Ochrona praw stron trzecich nie powinna jednak służyć za wymówkę dla uniemożliwiania osobom zgodnego z prawem dostępu. W takich przypadkach administrator powinien wdrożyć środki techniczne w celu realizacji żądania udzielenia dostępu (na przykład edycja obrazów, m.in. maskowanie lub randomizacja sekwencji bitowych). Administratorzy nie mają jednak obowiązku wdrożenia takich środków technicznych, jeżeli mogą w inny sposób zapewnić swoją gotowość do reagowania na wniosek zgodnie z art. 15, w terminie określonym w art. 12 ust. 3.

- Art. 11 ust. 2: administrator nie jest w stanie zidentyfikować osoby, której dane dotyczą

95. Jeżeli nie da się przeszukać nagrania wideo w celu odnalezienia danych osobowych (tj. administrator musiałby przeszukać znaczną ilość przechowywanych nagrań, aby znaleźć konkretną osobę, której dane dotyczą), administrator może nie być w stanie zidentyfikować osoby, której dane dotyczą.

96. Z tych względów osoba, której dane dotyczą, powinna (oprócz zidentyfikowania się za pomocą dokumentu tożsamości lub osobiście) we wniosku skierowanym do administratora sprecyzować, kiedy – w rozsądnym okresie/przedziale czasowym proporcjonalnym do ilości zarejestrowanych osób, których dane dotyczą – weszła na obszar objęty monitoringiem. Administrator powinien uprzednio powiadomić osobę, której dane dotyczą, o tym, jakie informacje są niezbędne do

zrealizowania wniosku przez administratora. Jeżeli administrator jest w stanie wykazać, że nie ma możliwości zidentyfikowania osoby, której dane dotyczą, administrator musi odpowiednio poinformować o tym osobę, której dane dotyczą, o ile jest to możliwe. W takiej sytuacji, w odpowiedzi udzielonej osobie, której dane dotyczą, administrator powinien zawrzeć informacje na temat konkretnego obszaru objętego monitoringiem, kontroli używanych kamer itd., aby osoba, której dane dotyczą, miała pełną świadomość tego, jakie jej dane osobowe mogły być przetwarzane.

Przykład: Jeżeli osoba, której dane dotyczą, składa wniosek o uzyskanie kopii swoich danych osobowych, przetwarzanych za pośrednictwem monitoringu wizyjnego przy wejściu do centrum handlowego, które dziennie odwiedza 30 000 osób, osoba, której dane dotyczą, powinna sprecyzować, kiedy znajdowała się na obszarze objętym monitoringiem mniej więcej w godzinowym okienku. Jeżeli administrator nadal przetwarza nagrania, należy dostarczyć kopię nagrania wideo. W przypadku gdy na tym samym nagraniu można zidentyfikować inne osoby, których dane dotyczą, wówczas ten fragment nagrania powinien zostać zanonimizowany (na przykład poprzez zamazanie obrazu kopii nagrania lub jego fragmentu) przed udostępnieniem kopii osobie, której dane dotyczą, która złożyła wniosek.

Przykład: Jeżeli administrator automatycznie usuwa wszystkie nagrania w ciągu na przykład dwóch dni, nie jest on w stanie dostarczyć nagrania osobie, której dane dotyczą, po upływie tego czasu. Jeżeli administrator otrzymuje wniosek po upływie dwóch dni, osoba, której dane dotyczą, powinna zostać o tym odpowiednio poinformowana.

97.

- Art. 12 RODO: nadmierne żądania

98. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, administrator może pobrać rozsądną opłatę zgodnie z art. 12 ust. 5 lit. a) RODO lub odmówić podjęcia działań w związku z żądaniem (art. 12 ust. 5 lit. b) RODO). Administrator musi być w stanie wykazać ewidentnie nieuzasadniony lub nadmierny charakter żądania.

6.2 Prawo do usunięcia danych i prawo do sprzeciwu

6.2.1 Prawo do usunięcia danych (prawo do bycia zapomnianym)

99. Jeżeli administrator nadal przetwarza dane osobowe, wykraczając poza monitorowanie w czasie rzeczywistym (np. przechowywanie), osoba, której dane dotyczą, może żądać usunięcia danych osobowych zgodnie z art. 17 RODO.

100. Na żądanie administrator ma obowiązek usunąć bez zbędnej zwłoki dane osobowe, w przypadku wystąpienia jednej z okoliczności wymienionych w art. 17 ust. 1 RODO (i w przypadku gdy nie występuje żaden z wyjątków określonych w art. 17 ust. 3 RODO). Dotyczy to obowiązku usunięcia danych osobowych, które nie są już niezbędne w celu, w którym zostały pierwotnie zebrane lub, w przypadku gdy przetwarzanie jest niezgodne z prawem (zob. również Rozdział 8 – okres przechowywania danych i obowiązek usunięcia danych). Ponadto w zależności od podstawy prawnej przetwarzania dane osobowe powinny zostać usunięte:

- *w przypadku zgody*, gdy zostaje ona wycofana (i nie istnieje żadna inna podstawa prawna przetwarzania),
- *w przypadku prawnie uzasadnionego interesu:*

- gdy tylko osoba, której dane dotyczą, korzysta z prawa do wniesienia sprzeciwu (zob. Rozdział 6.2.2) i nie istnieją żadne nadrzędne ważne, prawnie uzasadnione podstawy przetwarzania, lub
- w przypadku marketingu bezpośredniego (w tym profilowania), kiedy to osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania.

101. W przypadku upublicznienia nagrania wideo przez administratora (np. emisji lub transmisji strumieniowej w internecie na żywo) należy podjąć uzasadnione kroki w celu poinformowania innych administratorów (którzy obecnie przetwarzają dane osobowe) o żądaniu wniesionym zgodnie z art. 17 ust. 2 RODO. Takie uzasadnione kroki powinny obejmować środki techniczne, z uwzględnieniem dostępnych technologii i kosztu ich wdrożenia. W możliwie najszerszym zakresie administrator powinien powiadomić – po usunięciu danych osobowych – wszystkie osoby, którym uprzednio ujawniono dane osobowe, zgodnie z art. 19 RODO.

102. Oprócz obowiązku usunięcia danych osobowych ciążącego na administratorze, na żądanie osoby, której dane dotyczą, administrator jest zobowiązany na mocy ogólnych zasad określonych w RODO do ograniczenia przechowywanych danych osobowych (zob. *Rozdział 8*).

103. W przypadku monitoringu wizyjnego należy zauważyć, że, na przykład poprzez zamazanie obrazu bez możliwości odzyskania danych osobowych znajdujących się uprzednio na obrazie, dane osobowe uważa się za usunięte zgodnie z RODO.

> Przykład: Sklep spożywczy jest narażony na akty wandalizmu, szczególnie jego część zewnętrzna, w związku z czym na zewnątrz przed wejściem, bezpośrednio na ścianach zamontowano monitoring wizyjny. Przechodzień żąda usunięcia swoich danych osobowych utrwalonych na nagraniu w momencie, w którym przechodził obok sklepu. Administrator jest zobowiązany do uwzględnienia żądania bez zbędnej zwłoki i najpóźniej w terminie jednego miesiąca. Z uwagi na to, że dane nagranie nie służy już celowi, w jakim początkowo było przechowywane (nie odnotowano aktów wandalizmu w chwili, gdy osoba, której dane dotyczą, przechodziła obok sklepu), w chwili wniesienia żądania nie istnieje żaden prawnie uzasadniony interes dla przechowywania danych, który miałby nadrzędny charakter wobec interesów osób, których dane dotyczą. Administrator musi usunąć dane osobowe.

104.

6.2.2 Prawo do sprzeciwu

105. W przypadku monitoringu wizyjnego prowadzonego w oparciu o *prawnie uzasadniony interes* (art. 6 ust. 1 lit. f) RODO) lub konieczności przy wykonywaniu zadania w *interesie publicznym* (art. 6 ust. 1 lit. e) RODO) osoba, której dane dotyczą, ma prawo – w dowolnym momencie – do wniesienia sprzeciwu, z przyczyn związanych z jej szczególną sytuacją, wobec przetwarzania zgodnie z art. 21 RODO. Przetwarzanie danych osoby fizycznej musi zostać wstrzymane, chyba że administrator wykaże istnienie ważnych prawnie uzasadnionych podstaw, nadrzędnych wobec praw i interesów osoby, której dane dotyczą. Administrator jest zobowiązany do uwzględnienia żądania osoby, której dane dotyczą, bez zbędnej zwłoki i najpóźniej w terminie jednego miesiąca.

106. W kontekście monitoringu wizyjnego taki sprzeciw można wnieść wchodząc na obszar objęty monitoringiem, w trakcie lub po zakończeniu tego procesu. W praktyce oznacza to, że, o ile administrator nie ma ważnych prawnie uzasadnionych podstaw, monitorowanie danego obszaru, na którym możliwe byłoby zidentyfikowanie osób fizycznych, jest zgodne z prawem jedynie wówczas, gdy

(1) administrator może niezwłocznie zatrzymać przetwarzanie danych osobowych przez kamerę, o ile zgłoszono takie żądanie, lub

(2) dostęp do terenu objętego monitoringiem jest tak ograniczony, że administrator może zapewnić uzyskanie zgody od osoby, której dane dotyczą, przed jej wejściem na dany obszar, do którego osoba, której dane dotyczą, nie ma dostępu jako obywatel.

107. Niniejsze wytyczne nie służą określeniu co jest uznawane za *ważny* prawnie uzasadniony interes (art. 21 RODO).

108. W przypadku korzystania z monitoringu wizyjnego w celach marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo do wniesienia sprzeciwu wobec przetwarzania wedle własnego uznania, ponieważ prawo do sprzeciwu w tym kontekście ma charakter bezwzględny (art. 21 ust. 2 i 3 RODO).

> Przykład: Przedsiębiorstwo mierzy się z problemami dotyczącymi naruszeń bezpieczeństwa przy wejściu na jego teren i korzysta z monitoringu wizyjnego na podstawie prawnie uzasadnionego interesu w celu wychwycenia osób bezprawnie wchodzących na jego teren. Odwiedzający wnosi sprzeciw wobec przetwarzania swoich danych osobowych za pośrednictwem systemu monitoringu wizyjnego z przyczyn związanych z jego szczególną sytuacją. W tym przypadku przedsiębiorstwo nie uwzględnia żądania uzasadniając to faktem, że przechowywane nagranie jest niezbędne ze względu na toczące się dochodzenie wewnętrzne, posiadając tym samym ważne prawnie uzasadnione podstawy do tego, aby kontynuować przetwarzanie danych osobowych.

109.

7 PRZEJRZYSTOŚĆ I OBOWIĄZKI INFORMACYJNE[18]

110. Już od dawna nieodłącznym elementem europejskiego prawa o ochronie danych jest, aby osoby, których dane dotyczą, były świadome faktu działania monitoringu wizyjnego. Osoby te należy szczegółowo informować o miejscach objętych monitoringiem[19]. Zgodnie z RODO ogólne obowiązki w zakresie przejrzystości i obowiązki informacyjne określono w art. 12 RODO i nn. Wytyczne Grupy Roboczej art. 29 w sprawie przejrzystości na mocy rozporządzenia 2016/679 (WP260), które zostały zatwierdzone przez EROD w dniu 25 maja 2018 r., dostarczają dalszych szczegółów. Zgodnie z punktem 26 tychże wytycznych, to art. 13 RODO ma zastosowanie, w przypadku gdy dane osobowe pozyskiwane są „[...] od osoby, której one dotyczą, w drodze obserwacji (np. przy zastosowaniu automatycznych rejestratorów danych lub oprogramowania rejestrującego dane, np. kamer [...]".

111. W świetle ilości informacji, które należy dostarczyć osobie, której dane dotyczą, administratorzy danych mogą przyjąć podejście warstwowe, jeżeli zdecydują się na zastosowanie kombinacji metod w celu zapewnienia przejrzystości (WP260, pkt 35; WP89, pkt 22). Odnośnie monitoringu wizyjnego najważniejsze informacje powinny zostać umieszczone na samym znaku ostrzegawczym (pierwsza warstwa), a dalsze obowiązkowe szczegóły mogą być udostępnione za pośrednictwem innych środków (druga warstwa).

7.1 Informacje zawarte w pierwszej warstwie (znak ostrzegawczy)

112. Pierwsza warstwa dotyczy podstawowego sposobu, w jaki administrator po raz pierwszy wchodzi w interakcję z osobą, której dane dotyczą. Na tym etapie administratorzy muszą używać znaku ostrzegawczego przedstawiającego istotne informacje. Przedstawione informacje można opatrzyć znakami graficznymi, które w widoczny, zrozumiały i czytelny sposób przedstawią sens zamierzonego przetwarzania (art. 12 ust. 7 RODO). Format informacji należy dostosować do indywidualnej lokalizacji (WP89 pkt 22).

7.1.1 Umieszczenie znaku ostrzegawczego

113. Informacje należy umieścić w taki sposób, aby osoba, której dane dotyczą, mogła z łatwością stwierdzić obecność monitoringu przed wejściem na obszar objęty monitoringiem (mniej więcej na wysokości wzroku). Nie ma konieczności ujawniania miejsca, w którym umieszczono kamerę, o ile nie ma żadnych wątpliwości co do tego, które obszary zostały objęte monitoringiem, a kontekst monitoringu został jednoznacznie wyjaśniony (WP 89, pkt 22). Osoba, której dane dotyczą, musi być w stanie oszacować, który obszar jest obejmowany przez kamerę, aby mogła uniknąć objęcia monitoringiem lub odpowiednio dostosować swoje zachowanie, jeśli zaistnieje taka potrzeba.

7.1.2 Informacje zawarte w pierwszej warstwie

114. Pierwsza warstwa (znak ostrzegawczy) powinna zasadniczo przekazywać najważniejsze informacje, np. szczegóły dotyczące celów przetwarzania, tożsamości administratora i praw przysługujących osobie, której dane dotyczą, oraz najistotniejszych skutków przetwarzania[20]. Może ona obejmować, m.in. prawnie uzasadnione interesy administratora (lub strony trzeciej) oraz dane kontaktowe inspektora

[18] Zastosowanie mogą mieć szczególne wymogi określone w przepisach krajowych.

[19] Zob. WP89, Opinia 4/2004 w sprawie przetwarzania danych osobowych przy nadzorze z użyciem kamer video (Grupa Robocza Art. 29).

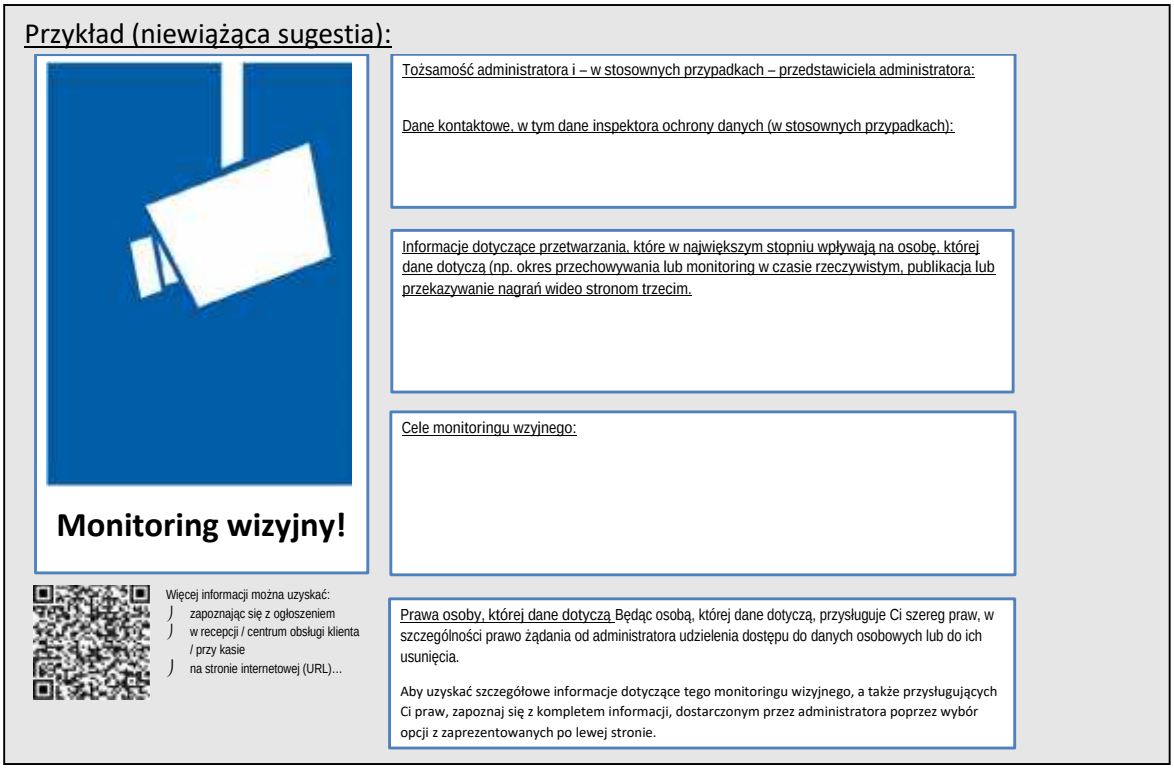
[20] Zob. WP260, pkt 38.

ochrony danych (w stosownych przypadkach). Musi się również odnosić do bardziej szczegółowej drugiej warstwy informacji oraz tego, gdzie i w jaki sposób ją znaleźć.

115. Ponadto znak powinien zawierać wszelkie informacje, które mogłyby stanowić zaskoczenie dla osoby, której dane dotyczą (WP260, pkt 38). Może to być na przykład przekazywanie danych stronom trzecim, zwłaszcza jeżeli są one zlokalizowane poza obszarem UE, a także okres przechowywania. W przypadku braku wskazania takich informacji osoba, której dane dotyczą, powinna mieć pewność, że uruchomiony jest tylko monitoring w czasie rzeczywistym (bez rejestrowania danych lub przekazywania danych stronom trzecim).

116.

Przykład (niewiążąca sugestia):



7.2 Informacje zawarte w drugiej warstwie

117. Drugą warstwę informacyjną również należy udostępnić w miejscu łatwo dostępnym dla osoby, której dane dotyczą, na przykład w formie kompletnego arkusza informacyjnego dostępnego w miejscu centralnym (np. w punkcie informacyjnym, przy recepcji lub przy kasie) lub przedstawić na łatwo dostępnym plakacie. Jak wspomniano powyżej pierwsza warstwa – znak ostrzegawczy – musi wyraźnie odnosić się do drugiej warstwy informacji. Ponadto najlepiej byłoby, jeżeli informacje pierwszej warstwy odnosiły się do źródła cyfrowego (np. kod QR lub adres strony internetowej) drugiej warstwy. Informacje te powinny być jednak łatwo dostępne nie tylko w formie cyfrowej. Powinna istnieć możliwość uzyskania dostępu do informacji drugiej warstwy bez wchodzenia na obszar objęty monitoringiem, zwłaszcza jeżeli informacje zostały udostępnione w formie cyfrowej (można to osiągnąć np. poprzez link). Inne odpowiednie środki mogą objąć numer telefonu, pod który można dzwonić. Bez względu na sposób dostarczenia informacji, muszą one zawierać wszelkie obowiązkowe elementy, o których mowa w art. 13 RODO.

118. Oprócz tych opcji, a także by zapewnić większą ich skuteczność, EROD zachęca do korzystania ze środków technicznych w celu dostarczenia informacji osobom, których dane dotyczą. Mogą one obejmować na przykład: kamery geolokalizujące oraz zawieranie informacji w aplikacjach mapowych lub na stronach internetowych, aby osoby mogły z jednej strony z łatwością zidentyfikować i określić źródła wideo, związane z wykonywaniem przysługujących im praw, a z drugiej strony uzyskać bardziej szczegółowe informacje dotyczące procesu przetwarzania.

> Przykład: Właściciel sklepu monitoruje swój sklep. Aby spełnić wymogi określone w art. 13, wystarczy przy wejściu do sklepu w widocznym miejscu umieścić znak ostrzegawczy, który zawiera informacje pierwszej warstwy. Ponadto musi on udostępnić arkusz informacyjny zawierający informacje drugiej warstwy przy kasie lub w innym centralnym i łatwo dostępnym miejscu w sklepie.

119.

8 OKRESY PRZECHOWYWANIA I OBOWIĄZEK USUNIĘCIA DANYCH

120. Danych osobowych nie można przechowywać przez okres dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane (art. 5 ust. 1 lit. c) i e) RODO). W niektórych państwach członkowskich mogą istnieć przepisy szczegółowe dotyczące okresów przechowywania w związku z monitoringiem wizyjnym, zgodnie z art. 6 ust. 2 RODO.

121. To, czy istnieje konieczność przechowywania danych, czy też nie, powinno podlegać kontroli w krótkim okresie. Co do zasady prawnie uzasadnione cele prowadzenia monitoringu wizyjnego to często ochrona mienia lub zabezpieczenie materiału dowodowego. Powstałe szkody można zazwyczaj stwierdzić w ciągu jednego lub dwóch dni. Aby umożliwić wykazanie zgodności z ramami prawnymi ochrony danych, w interesie administratora leży dokonanie uprzednich ustaleń organizacyjnych (np. wyznaczenie, w stosownych przypadkach, osoby odpowiedzialnej za przegląd i zabezpieczenie nagrań wideo). Uwzględniając zasady określone w art. 5 ust. 1 lit. c) i e) RODO, a mianowicie minimalizacji danych i ograniczenia przechowywania, w większości przypadków (np. dla celu wykrycia aktów wandalizmu) dane osobowe powinny zostać usunięte, najlepiej automatycznie, po kilku dniach. Im dłuższy okres przechowywania (zwłaszcza, gdy przekracza on 72 godziny), tym więcej należy przedstawić argumentów przemawiających za zgodnością z prawem celu i konieczności przechowywania. W przypadku gdy administrator korzysta z monitoringu wizyjnego nie tylko w celu monitorowania swojej nieruchomości, lecz zamierza również przechowywać dane, administrator musi zapewnić, aby przechowywanie to było rzeczywiście niezbędne do osiągnięcia założonego celu. W takim przypadku należy wyraźnie wskazać okres przechowywania i określić go indywidualnie dla każdego celu. Do obowiązków administratora należy określenie okresu przechowywania zgodnie z zasadami konieczności (niezbędności) i proporcjonalności, a także wykazanie zgodności z przepisami RODO.

> Przykład: Właściciel małego sklepu zapewne zauważyłby wszelkie akty wandalizmu już w dniu, w którym ich dokonano. A zatem normalny okres przechowywania wynoszący 24 godziny jest wystarczająco długi. Weekendy i dni wolne od pracy mogłyby jednak przemawiać za dłuższym okresem przechowywania. W przypadku wykrycia jakichkolwiek szkód właściciel prawdopodobnie będzie musiał przechowywać nagranie wideo przez dłuższy okres, w celu wszczęcia postępowania przeciwko sprawcy przestępstwa.

122.

9 ŚRODKI TECHNICZNE I ORGANIZACYJNE

123. Jak określono w art 32 ust. 1 RODO, przetwarzanie danych osobowych w trakcie działania monitoringu wizyjnego musi być nie tylko dozwolone z prawnego punktu widzenia, lecz także administratorzy i podmioty przetwarzające muszą je odpowiednio zabezpieczyć. Wdrożone **środki techniczne i organizacyjne** muszą być **proporcjonalne do zagrożeń stwarzanych wobec praw i wolności osób fizycznych**, wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych pochodzących z monitoringu wizyjnego. Zgodnie z art. 24 i art. 25 RODO administratorzy muszą wdrożyć środki techniczne i organizacyjne, aby zapewnić stosowanie wszelkich zasad dotyczących ochrony danych w trakcie ich przetwarzania i ustanowić środki dla osób, których dane dotyczą, umożliwiające wykonywanie ich praw, o których mowa w art. 15–22 RODO. Administratorzy danych powinni przyjąć wewnętrzne ramy i polityki, aby zapewnić takie wdrażanie zarówno w chwili określania

środków przetwarzania, jak i w czasie samego przetwarzania, w tym przeprowadzenia oceny skutków dla ochrony danych, w razie potrzeby.

9.1 Przegląd systemu monitoringu wizyjnego

124. Na system monitoringu wizyjnego (SMW)[21] składają się urządzenia analogowe i cyfrowe, jak również oprogramowanie służące utrwalaniu obrazów, ich przetwarzaniu i wyświetlaniu operatorowi. Jego składniki zostały pogrupowane w następujące kategorie:

- Środowisko wizualne: utrwalanie obrazu, wzajemne połączenia i przetwarzanie obrazów;
  - celem utrwalania obrazu jest tworzenie obrazu otaczającej rzeczywistości w takim formacie, który może zostać wykorzystany przez pozostałe funkcje systemu,
  - wzajemne połączenia odnoszą się do wszystkich środków przesyłania danych w obrębie środowiska wizualnego, tj. łącza i komunikacja. Przykładami łączy są kable, sieci cyfrowe i transmisje bezprzewodowe. Komunikacja odnosi się do wszystkich sygnałów danych wideo i danych kontrolnych, które mogą być cyfrowe lub analogowe,
  - przetwarzanie obrazów obejmuje analizę, przechowywanie i prezentację obrazu lub sekwencji obrazów.
- Z perspektywy zarządzania systemem, SMW posiada następujące funkcje logiczne:
  - zarządzanie danymi i zarządzanie działaniami, które obejmują obsługę poleceń operatora oraz działania generowane przez system (procedury alarmowe, podmioty alarmujące),
  - interfejsy innych systemów mogą obejmować połączenia z innymi systemami bezpieczeństwa (kontrola dostępu, alarm pożarowy) oraz systemami niezwiązanymi z bezpieczeństwem (tworzenie systemów zarządzania, automatyczne rozpoznawanie tablic rejestracyjnych).
- Na bezpieczeństwo SMW składa się poufność, integralność i dostępność systemu i danych:
  - bezpieczeństwo systemu obejmuje bezpieczeństwo fizyczne wszystkich elementów systemu i kontrolę dostępu do SMW,
  - bezpieczeństwo danych obejmuje zapobieganie utracie lub manipulacji danych.

[21] RODO nie zawiera żadnej definicji, techniczny opis można zaleźć, na przykład w EN 62676-1-1:2014 Systemy dozorowe CCTV stosowane w zabezpieczeniach – część 1–1: Wymogi dotyczące systemu wideo.

125.

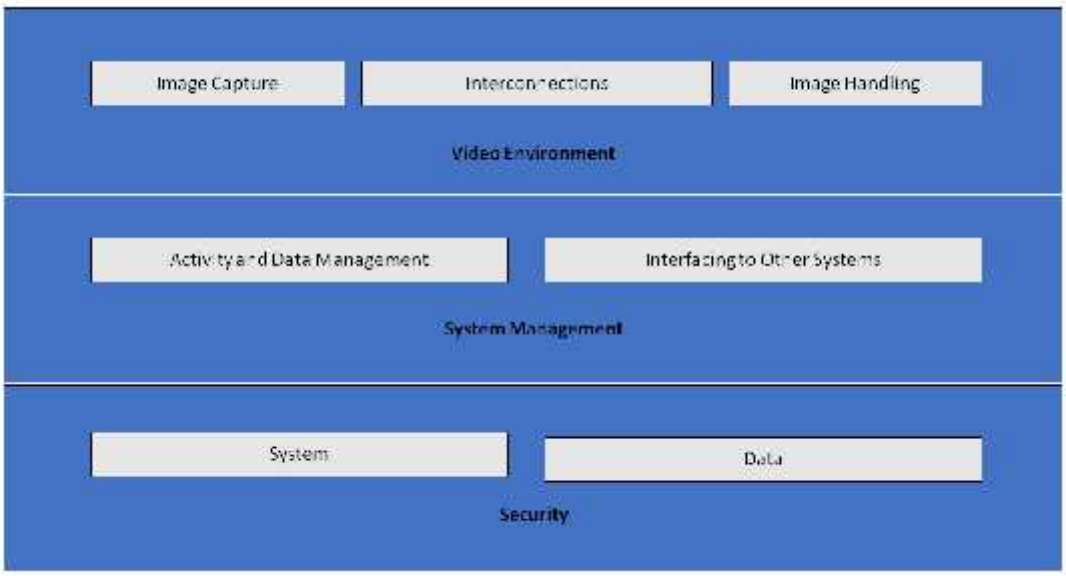


Image Capture	Utrwalanie obrazu
Interconnections	Wzajemne połączenia
Image Handling	Przetwarzanie obrazów
Video Environment	Środowisko wizualne
Activity and Data Management	Zarządzanie działaniami i danymi
Interfacing to Other Systems	Połączenia z innymi systemami
System Management	Zarządzanie systemem
System	System
Data	Dane
Security	Bezpieczeństwo

Rys. 1 – system monitoringu wizyjnego

9.2 Ochrona danych w fazie projektowania oraz domyślna ochrona danych

126. Jak określono w art. 25 RODO, administratorzy muszą wdrożyć odpowiednie środki techniczne i organizacyjne w zakresie ochrony danych już w fazie planowania monitoringu wizyjnego – przed rozpoczęciem gromadzenia i przetwarzania nagrań wideo. Zasady te podkreślają potrzebę wbudowanych technologii służących wzmocnieniu ochrony prywatności, ustawień domyślnych, które minimalizują przetwarzanie danych, oraz zapewnienia niezbędnych narzędzi umożliwiających jak najlepszą ochronę danych osobowych[22].

127. Administratorzy powinni tworzyć zabezpieczenia służące ochronie danych i prywatności nie tylko w ramach specyfikacji technicznych projektu, lecz również praktyk organizacyjnych. Jeżeli chodzi o praktyki organizacyjne, administrator powinien przyjąć odpowiednie ramy zarządzania, ustanowić i realizować polityki i procedury dotyczące monitoringu wizyjnego. Z technicznego punktu widzenia specyfikacja i projekt systemu powinny obejmować wymogi w zakresie przetwarzania danych osobowych zgodnie z zasadami określonymi w art. 5 RODO (zgodność przetwarzania z prawem, ograniczenie celu i danych, domyślna minimalizacja danych w rozumieniu art. 25 ust. 2 RODO,

[22]Opinia WP 168 w sprawie „Przyszłości prywatności”, wspólny wkład Grupy Roboczej Art. 29 i Grupy Roboczej ds. Policji i Wymiaru Sprawiedliwości do Konsultacji Komisji Europejskiej w sprawie ram prawnych dla podstawowego prawa do ochrony danych osobowych (przyjęta w dniu 1 grudnia 2009 r.).

integralność i poufność danych, rozliczalność itd.). W przypadku gdy administrator planuje nabyć komercyjny system monitoringu wizyjnego, musi on zawrzeć te wymogi w specyfikacji zakupu. Administrator musi zapewnić zgodność z tymi wymogami, stosując je w odniesieniu do wszystkich elementów składowych systemu i do wszystkich danych przetwarzanych w ramach tego systemu w trakcie całego cyklu ich życia.

9.3 Konkretne przykłady odpowiednich środków

128. Większość środków, które mogą służyć zabezpieczeniu monitoringu wizyjnego, zwłaszcza w przypadku wykorzystania sprzętu i oprogramowania cyfrowego, nie będzie się różnić od tych, które zostały wykorzystane w innych systemach informatycznych. Niemniej, bez względu na wybrane rozwiązanie, administrator musi odpowiednio chronić wszystkie składniki systemu monitoringu wizyjnego oraz dane na wszystkich etapach, tj. w trakcie przechowywania (dane nieaktywne), przesyłania (dane przesyłane) i przetwarzania (dane wykorzystywane). W tym celu niezbędne jest, by administratorzy i podmioty przetwarzające łączyli środki techniczne i organizacyjne.

129. Przy wyborze rozwiązań technicznych administrator powinien rozważyć wprowadzenie technologii chroniących prywatność, również dlatego że zwiększają one bezpieczeństwo. Przykładami takich technologii są systemy umożliwiające maskowanie lub randomizację sekwencji bitowych obszarów, które pozostają bez znaczenia dla monitoringu, a także usunięcie wizerunku osób trzecich przed dostarczeniem nagrania wideo osobom, których dane dotyczą[23]. Z drugiej strony wybrane rozwiązania nie powinny zawierać funkcji, które nie są niezbędne (np. nieograniczone ruchy kamery, możliwość przybliżenia, transmisja radiowa, analiza i nagrania dźwiękowe). Funkcje, które są dostępne i nie są niezbędne, należy dezaktywować.

130. Istnieje wiele materiałów na ten temat, w tym międzynarodowe normy i specyfikacje techniczne w zakresie bezpieczeństwa fizycznego systemów multimedialnych[24] oraz ogólnego bezpieczeństwa systemów informatycznych[25]. W związku z tym sekcja ta zawiera jedynie przegląd kluczowych zagadnień dotyczących tego tematu.

9.3.1 Środki organizacyjne

131. Oprócz potencjalnie niezbędnej oceny skutków dla ochrony danych (zob. Rozdział 10) administratorzy powinni wziąć pod uwagę następujące wątki przy tworzeniu swoich polityk i procedur w zakresie monitoringu wizyjnego:

- Kto odpowiada za zarządzanie i obsługę systemu monitoringu wizyjnego.
- Cel i zakres projektu monitoringu wizyjnego.
- Właściwe i niedozwolone wykorzystanie (w jakich miejscach i w jakim czasie wykorzystanie monitoringu wizyjnego jest dozwolone, a kiedy i gdzie nie jest; np. wykorzystanie ukrytych kamer i nagrań dźwiękowych oprócz nagrań wideo)[26].

---

[23] W niektórych przypadkach wykorzystanie takich technologii może być obowiązkowe w celu spełnienia wymogów, o których mowa w art. 5 ust. 1 lit. c). W każdym razie mogą one posłużyć jako przykłady najlepszych praktyk.

[24] IEC TS 62045 – Bezpieczeństwo multimedialne – Wskazówki dotyczące ochrony prywatności używanego i nieużywanego sprzętu oraz systemów.

[25] ISO/IEC 27000 – Seria „Systemy zarządzania bezpieczeństwem informacji".

[26] Może to być uzależnione od przepisów krajowych i regulacji dotyczących danego sektora.

- Środki służące przejrzystości, o których mowa w Rozdziale 7 (*Przejrzystość i obowiązki informacyjne*).
- W jaki sposób rejestruje się nagrania wideo i na jaki czas, uwzględniając okres archiwizacji nagrań wideo związany z incydentami bezpieczeństwa.
- Kto musi przejść odpowiednie szkolenie i kiedy.
- Kto ma dostęp do nagrań wideo i w jakich celach.
- Procedury operacyjne (np. kto i z jakiego miejsca sprawuje nadzór nad monitoringiem wizyjnym, jak postępować w przypadku naruszenia ochrony danych).
- Do jakich procedur wnioskowania o uzyskanie dostępu do nagrań wideo muszą stosować się strony zewnętrzne oraz procedury dotyczące odrzucenia lub uznania wniosku.
- Procedury dotyczące zamówienia, instalacji i konserwacji SMW.
- Procedury zarządzania incydentami oraz odzyskiwania danych.

9.3.2 Środki techniczne

132. **Bezpieczeństwo systemu** oznacza **bezpieczeństwo fizyczne** wszystkich elementów składowych systemu i integralność systemu, tj. **ochronę przed umyślną i nieumyślną ingerencją w normalne działania systemu i odporność na nią** oraz **kontrolę dostępu**. Bezpieczeństwo danych oznacza **poufność** (dane są dostępne wyłącznie dla osób, którym przyznano dostęp), **integralność** (zapobieganie utracie lub manipulowaniu danych) oraz **dostępność** (można uzyskać dostęp do danych, gdy jest to wymagane).

133. **Bezpieczeństwo fizyczne** stanowi istotny element ochrony danych oraz pierwszą linię obrony, ponieważ zapobiega przed kradzieżą sprzętu SMW, aktami wandalizmu, klęskami żywiołowymi, katastrofami spowodowanymi przez człowieka i przypadkowymi uszkodzeniami (np. w wyniku przepięcia, ekstremalnych temperatur, czy też rozlanej kawy). W przypadku systemu analogowego bezpieczeństwo fizyczne odgrywa główną rolę w zapewnieniu ich ochrony.

134. **Bezpieczeństwo systemu i danych**, tzn. ochrona przed umyślną i nieumyślną ingerencją w jego normalne działania, może obejmować:

- ochronę całej infrastruktury SMW (w tym kamery zdalnie sterowane, okablowanie i zasilanie) przed fizyczną ingerencją i kradzieżą,
- ochronę przesyłania nagrań wideo za pośrednictwem kanałów komunikacyjnych zabezpieczonych przed przechwytywaniem danych,
- szyfrowanie danych,
- korzystanie z rozwiązań opartych na wykorzystaniu sprzętu i oprogramowania, takich jak zapory sieciowe, systemy antywirusowe i systemy wykrywania włamań, chroniące przed cyberatakami,
- wykrywanie awarii elementów składowych, oprogramowania i wzajemnych połączeń,
- środki służące odzyskiwaniu dostępności i dostępu do systemu w razie incydentu fizycznego lub technicznego.

135. **Kontrola dostępu** gwarantuje, że tylko osoby upoważnione będą miały dostęp do systemu i danych, podczas gdy pozostałe osoby są takiej możliwości pozbawione. Środki wspierające kontrolę dostępu fizycznego i logicznego obejmują:

- Zapewnienie zabezpieczenia wszystkich obiektów objętych monitoringiem wizyjnym i w których przechowywane są nagrania wideo, przed niekontrolowanym dostępem przez strony trzecie.

- Ustawienie monitorów w taki sposób (zwłaszcza jeżeli znajdują się one w przestrzeniach otwartych, takich jak recepcja), aby ich ekrany mogły być widoczne jedynie dla upoważnionych operatorów.
- Określono i wdrożono procedury w zakresie przyznania, zmiany i wycofania dostępu fizycznego i logicznego.
- Wdrożono metody i środki uwierzytelniania i autoryzacji użytkowników, obejmujące m.in. długość haseł i częstotliwość ich zmiany.
- Działania użytkowników (zarówno w odniesieniu do systemu, jak i danych) są rejestrowane i poddawane regularnym przeglądom.
- Problemy z dostępem są na bieżąco monitorowane i identyfikowane, a wykryte podatności są rozwiązywane możliwie jak najszybciej.

10 OCENA SKUTKÓW DLA OCHRONY DANYCH

136. Zgodnie z art. 35 ust. 1 RODO administratorzy są zobowiązani do przeprowadzenia oceny skutków dla ochrony danych (DPIA), w przypadku gdy dany rodzaj przetwarzania danych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Art. 35 ust. 3 lit. c) RODO stanowi, że administratorzy mają obowiązek przeprowadzenia ocen skutków dla ochrony danych, jeżeli przetwarzanie stanowi systematyczne monitorowanie miejsca dostępnego publicznie na dużą skalę. Ponadto zgodnie z art. 35 ust. 3 lit. b) RODO należy również przeprowadzić ocenę skutków dla ochrony danych, w przypadku gdy administrator zamierza przetwarzać szczególne kategorie danych na dużą skalę.

137. Wytyczne dotyczące oceny skutków dla ochrony danych[27] zawierają dalsze wskazówki i bardziej szczegółowe przykłady odnoszące się do monitoringu wizyjnego (np. dotyczące „wykorzystywania systemu kamer w celu monitorowania zachowania kierowców na autostradach"). Zgodnie z art. 35 ust. 4 RODO wszystkie organy nadzorcze są zobowiązane do opublikowania wykazu rodzaju operacji przetwarzania podlegających obowiązkowemu przeprowadzeniu oceny skutków dla ochrony danych (DPIA) w ich państwie. Wykazy te można zwykle znaleźć na stronach internetowych organów. Biorąc pod uwagę typowe cele monitoringu wizyjnego (ochrona osób i mienia, wykrywanie przestępstw, zapobieganiem im oraz ich kontrola, gromadzenie materiału dowodowego i identyfikacja biometryczna podejrzanych), zasadne jest założenie, że w wielu przypadkach dotyczących monitoringu wizyjnego konieczne będzie przeprowadzenie oceny skutków dla ochrony danych. Dlatego też administratorzy danych powinni uważnie zapoznać się z tymi dokumentami, aby stwierdzić, czy istnieje konieczność przeprowadzenia takiej oceny i przeprowadzić ją, jeśli to niezbędne. Wybór administratora w zakresie wdrażanych środków ochrony danych powinien być podyktowany wynikiem przeprowadzonej oceny skutków dla ochrony danych.

138. Należy również zauważyć, że jeśli wyniki oceny skutków dla ochrony danych wskazują, że przetwarzanie stanowiłoby wysokie ryzyko pomimo planowanego wdrożenia środków bezpieczeństwa przez administratora, wówczas konieczne będzie skonsultowanie się z odpowiednim organem nadzorczym przed rozpoczęciem przetwarzania. Szczegóły dotyczące uprzednich konsultacji można znaleźć w art. 36.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)

[27] WP248 rev.01, Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko", do celów rozporządzenia 2016/679. – zatwierdzone przez EROD