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

Wersja 2.0

przyjęta w dniu 29 stycznia 2020 r.

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Historia wersji

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

1 Wprowadzenie 5

2 Zakres stosowania 7

2.1 Dane osobowe 7

2.2 Stosowanie dyrektywy o ochronie danych w sprawach karnych (UE2016/680) 7

2.3 Wyjątek dla gospodarstw domowych 8

3 Zgodność przetwarzania z prawem 9

3.1 Prawnie uzasadniony interes, art. 6 ust. 1 lit. f) 9

3.1.1 Istnienie prawnie uzasadnionych interesów 9

3.1.2 Konieczność przetwarzania 10

3.1.3 Wyważenie interesów 11

3.2 Konieczność realizacji zadania wykonywanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 6 ust. 1 lit. e)) 14

3.3 Zgoda, art. 6 ust. 1 lit. a) 14

4 Ujawnienie nagrań wideo stronom trzecim 16

4.1 Ujawnienie nagrań wideo stronom trzecim – zarys 16

4.2 Ujawnienie nagrań wideo organom ścigania 16

5 Przetwarzanie szczególnych kategorii danych 18

5.1 Względy ogólne dotyczące przetwarzania danych biometrycznych 19

5.2 Proponowane środki minimalizujące ryzyko przy przetwarzaniu danych biometrycznych .. 22

6 Prawa osoby, której dotyczą dane 24

6.1 Prawo dostępu 24

6.2 Prawo do usunięcia danych i prawo do sprzeciwu 25

6.2.1 Prawo do usunięcia danych (prawo do bycia zapomnianym) 25

6.2.2 Prawo do sprzeciwu 26

7 Przejrzystość i obowiązki informacyjne 28

7.1 Informacje zawarte w pierwszej warstwie (znak ostrzegawczy) 28

7.1.1 Umieszczenie znaku ostrzegawczego 28

7.1.2 Informacje zawarte w pierwszej warstwie 28

7.2 Informacje zawarte w drugiej warstwie 29

8 Okresy przechowywania i obowiązek usunięcia danych 31

9 Środki techniczne i organizacyjne 31

9.1 Przegląd systemu monitoringu wizyjnego 32

9.2 Ochrona danych w fazie projektowania oraz domyślna ochrona danych 33

9.3 Konkretne przykłady odpowiednich środków 34

9.3.1 Środki organizacyjne 34
9.3.2 Środki techniczne 35
10 Ocena skutków dla ochrony danych 37

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. Częstsze korzystanie z urządzeń wideo wpływa na zachowanie obywateli. Wzmożone wysiłki na rzecz wdrażania takich narzędzi w różnych sferach życia osób fizycznych będzie w jeszcze większym stopniu skłaniało je do zapobiegania wykryciu ewentualnych anomalii. Tak naprawdę technologie te mogą ograniczać możliwości anonimowego przemieszczania się oraz korzystania z usług i generalnie ograniczać możliwość pozostania niezauważonym. Wpływ na ochronę danych jest ogromny.

2. Mimo iż osoby fizyczne mogą nie mieć nic przeciwko monitoringowi wizyjnemu zainstalowanemu na przykład w określonym celu związanym z bezpieczeństwem, należy ustanowić zabezpieczenia, aby uniknąć wykorzystania danych niezgodnie z przeznaczeniem w zupełnie innych – dla osób, których dane dotyczą – i nieoczekiwanych celach (np. w celach marketingowych, monitorowania wyników 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 zwiększają ryzyko ich wtórnego wykorzystania (bez względu na to, czy są związane z celem pierwotnie przypisanym systemowi) lub nawet ryzyko związane z wykorzystaniem danych niezgodnie z przeznaczeniem. Zawsze należy dokładnie przeanalizować ogólne zasady określone w RODO (art. 5) mając do czynienia z monitoringiem wizyjnym.

3. Systemy monitoringu wizyjnego pod wieloma względami zmieniają sposób, w jaki specjaliści z sektora prywatnego i publicznego współpracują ze sobą w miejscach prywatnych i publicznych w celu zwiększenia bezpieczeństwa, uzyskania analizy oglądalności, dostarczenia spersonalizowanych reklam itd. Monitoring wizyjny stał się wysoce skuteczny za sprawą wdrażania inteligentnej analizy obrazu na coraz większą skalę. Metody te mogą być bardziej (np. złożone technologie biometryczne) lub mniej inwazyjne (np. proste algorytmy liczenia). Co do zasady pozostanie anonimowym oraz zachowanie prywatności staje się coraz trudniejsze. Poruszone kwestie związane z ochroną danych mogą różnić się

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

w zależności od sytuacji, dotyczy to również analizy prawnej przy korzystaniu z którejkolwiek z tych technologii.

4. Oprócz kwestii prywatności istnieją również ryzyka związane z ewentualnym nieprawidłowym działaniem tych urządzeń oraz związanych z tym uprzedzeń. 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 uprzedzenia związane z rozpoznawaniem twarzy stwarzają ryzyko pogłębienia uprzedzeń wśród społeczeństwa. Dlatego też administratorzy danych muszą również zapewnić, aby przetwarzanie danych biometrycznych pochodzących z monitoringu wizyjnego podlegało regularnej ocenie jego znaczenia i skuteczności zastosowanych zabezpieczeń.

5. Nie ma konieczności korzystania wyłącznie z monitoringu wizyjnego, ponieważ istnieją inne środki umożliwiające osiągnięcie podstawowego celu. W innym przypadku mierzymy się z ryzykiem zmian w zakresie norm kulturowych prowadzących do zaakceptowania braku prywatności już od samego początku.

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, można zastosować ogólne rozumowanie w odniesieniu do wszystkich potencjalnych obszarów użytkowania.

2 ZAKRES STOSOWANIA[2]

2.1 Dane osobowe

7. W obecnych czasach systematyczny zautomatyzowany monitoring konkretnego terenu za pomocą środków optycznych lub audiowizualnych, głównie w celu ochrony mienia lub ochrony życia i zdrowia osoby fizycznej, stał się powszechnym zjawiskiem. Działanie to wiąże się z gromadzeniem i przechowywaniem informacji graficznych lub audiowizualnych dotyczących wszystkich osób wchodzących na monitorowany teren, które można zidentyfikować na podstawie ich wyglądu lub innych cech szczególnych. Dane te często umożliwiają ustalenie tożsamości tych osób. Monitoring umożliwia również dalsze przetwarzanie danych osobowych dotyczących obecności osób i ich zachowania na danym terenie. Potencjalne ryzyko wykorzystania danych niezgodnie z przeznaczeniem zwiększa się wraz z wielkością monitorowanego obszaru, jak również z liczbą osób przebywających na tym obszarze. Fakt ten potwierdza art. 35 ust. 3 lit. c) ogólnego rozporządzenia o ochronie danych, w którym nakłada się obowiązek przeprowadzenia oceny skutków dla ochrony danych w przypadku systematycznego monitorowania na dużą skalę miejsca dostępnego publicznie, jak również art. 37 ust. 1 lit. b), w którym nakłada się na podmioty przetwarzające obowiązek wyznaczenia inspektora ochrony danych, w przypadku gdy proces przetwarzania, ze względu na swój charakter, wiąże się z regularnym i systematycznym monitorowaniem osób, których dane dotyczą.

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

> Przykład: RODO nie ma zastosowania do atrap kamer (tj. kamer, które nie działają zgodnie ze swoim przeznaczeniem i w związku z tym nie przetwarzają żadnych danych osobowych). *W niektórych państwach członkowskich rozporządzenie to może jednak podlegać innym przepisom.*
>
> Przykład: Nagrania wykonane na dużych wysokościach wchodzą w zakres stosowania RODO wyłącznie 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 zbudowana 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 o ochronie danych w sprawach karnych (UE2016/680)

10. W zakres stosowania dyrektywy (UE) 2016/680 wchodzi zwłaszcza przetwarzanie danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, ich wykrywania lub ścigania lub wykonywania kar kryminalnych, w tym 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 dla gospodarstw domowych

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

12. Należy przyjąć wąską interpretację niniejszego przepisu – tzw. wyjątku dla gospodarstw domowych – w kontekście monitoringu wizyjnego. Jak zatem uznał Trybunał Sprawiedliwości Unii Europejskiej tzw. „wyjątek dla gospodarstw domowych" 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, o ile 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 sterowane na prywatnej posiadłości danej osoby, mogą one być objęte wyjątkiem dla gospodarstw domowych. Będzie to uzależnione od wielu różnych czynników, które należy w pełni rozważyć, aby wyciągnąć odpowiednie wnioski. Poza wyżej wymienionymi elementami wskazanymi w orzeczeniach TSUE użytkownik monitoringu wizyjnego o charakterze domowym musi rozważyć, czy łączą go jakiekolwiek relacje z osobą, której dane dotyczą, czy skala i częstotliwość monitoringu wskazują na jakąkolwiek działalność zawodową z jego strony, a także potencjalny negatywny wpływ monitoringu na osoby, których dane dotyczą. Obecność któregokolwiek z wyżej wymienionych elementów niekoniecznie sugeruje, że przetwarzanie wykracza poza zakres wyjątku dla gospodarstw domowych: aby to stwierdzić, należy dokonać ogólnej oceny.

> Przykład: Turysta nagrywa film zarówno telefonem komórkowym, jak i kamerą, aby udokumentować swoje wakacje. Pokazuje nagranie przyjaciołom i rodzinie, lecz nie udostępnia go nieograniczonej liczbie osób. Taka sytuacja byłaby objęta wyjątkiem dla gospodarstw domowych.
>
> Przykład: Kobieta uprawiająca kolarstwo górskie chce nagrać swój zjazd kamerą sportową. Jeździ ona w oddalonym regionie i zamierza wykorzystać te nagrania wyłącznie w celach osobistych i domowych. Taka sytuacja byłaby objęta wyjątkiem dla gospodarstw domowych, nawet jeżeli dane osobowe byłyby do pewnego stopnia przetwarzane.
>
> Przykład: Ktoś monitoruje i nagrywa swój własny ogród. Nieruchomość jest ogrodzona i tylko sam administrator oraz jego rodzina przebywają w tym ogrodzie na co dzień. Taka sytuacja byłaby objęta wyjątkiem dla gospodarstw domowych, pod warunkiem że monitoring wizyjny nie rozciąga się choćby 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)). Monitoring wizyjny może być wykorzystywany do różnych celów, np. zwiększenia ochrony mienia i majątku, zwiększenia ochrony życia i integralności cielesnej osób fizycznych, gromadzenia dowodów w sprawach cywilnych[6]. Te cele monitorowania należy udokumentować na piśmie (art. 5 ust. 2) i określić w odniesieniu do każdej kamery używanej do monitorowania wizyjnego. Informacje na temat kamer wykorzystywanych w tym samym celu przez jednego administratora danych można udokumentować w ramach jednej operacji. Ponadto należy poinformować osoby, których dane dotyczą, o celu lub celach przetwarzania zgodnie z art. 13 (*zob. Sekcja 7, Przejrzystość i obowiązki informacyjne*). Monitoring wizyjny wykorzystywany wyłącznie do celów „bezpieczeństwa" lub „własnego bezpieczeństwa" nie jest pojęciem wystarczająco precyzyjnym (art. 5 ust. 1 lit. b)). Ponadto jest on sprzeczny z zasadą stanowiącą, że dane osobowe są przetwarzane w sposób zgodny z prawem, przejrzysty i uczciwy odnośnie do 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) (konieczność 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 konieczny do osiągnięcia celu prawnie uzasadnionego interesu administratora danych lub strony trzeciej, chyba że interesy te są podrzędne w stosunku do interesów osób, których dane dotyczą, lub podstawowych praw i wolności (art. 6 ust. 1 lit. f)). Prawnie uzasadnione interesy administratora lub strony trzeciej mogą stanowić interesy prawnie uzasadnione[8], gospodarcze lub niematerialne[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 osoby, której dane dotyczą, wyłącznie

[6] Przepisy dotyczące gromadzenia dowodów w sprawach 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, wyrok w sprawie C–13/16, sprawa Rigas satiksme, z dnia 4 maja 2017 r.

[9] Zob. WP217, Grupa Robocza 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 ustanowienia, wykonania i ochrony roszczeń prawnych.

19. Biorąc pod uwagę realną i niebezpieczną sytuację cel polegający na ochronie nieruchomości przed włamaniem, kradzieżą lub aktami wandalizmu może stanowić prawnie uzasadniony interes przemawiający za zastosowaniem monitoringu wizyjnego.

20. Prawnie uzasadniony interes musi mieć wymiar realny i stanowić kwestię bieżącą (tj. nie może być fikcyjny lub spekulacyjny)[10]. Przed rozpoczęciem monitoringu musi zaistnieć sytuacja rzeczywistego zagrożenia – np. szkody lub poważne incydenty mające miejsce w przeszłości. Zgodnie z zasadą rozliczalności, administratorzy powinni dokumentować istotne incydenty (datę, sposób, 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 uważa się za 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 Konieczność 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 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 uzasadnione 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 nieruchomość.

27. Ogólnie rzecz biorąc konieczność korzystania z monitoringu wizyjnego w celu ochrony nieruchomości administratorów ustaje wzdłuż granic wyznaczających teren ich nieruchomości.[11] Niemniej istnieją przypadki, w których monitorowanie nieruchomości nie jest wystarczającym środkiem zapewniającym skuteczną ochronę. W niektórych indywidualnych przypadkach konieczne może okazać się rozszerzenie zakresu monitoringu wizyjnego, aby objął swoim zasięgiem bezpośrednie sąsiedztwo nieruchomości. W tym kontekście administrator powinien wziąć pod uwagę środki fizyczne i techniczne, na przykład blokowanie wyświetlania 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 obiektów lub miejsc dostępnych publicznie znajdujących się w sąsiedztwie księgarni.

28.

29. Pytania dotyczące konieczności przetwarzania pojawiają się również w odniesieniu do sposobu przechowywania dowodów. W niektórych przypadkach niezbędne może być zastosowanie rozwiązań polegających na wykorzystaniu czarnych skrzynek, w przypadku których nagranie jest automatycznie usuwane po upływie określonego okres przechowywania i dostępne wyłącznie w przypadku wystąpienia incydentu. W innych sytuacjach rejestrowanie plików wideo może w ogóle nie być konieczne, a bardziej odpowiednim rozwiązaniem byłoby wykorzystanie monitorowania w czasie rzeczywistym. Decyzja między wyborem rozwiązania polegającego na wykorzystaniu czarnych skrzynek a monitoringiem w czasie rzeczywistym powinna być uzależniona od założonego celu. Na przykład jeżeli celem monitoringu wizyjnego jest zabezpieczenie dowodów, metody w czasie rzeczywistym zazwyczaj nie są 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 czarnych skrzynkach). 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, którzy są 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 prawnie uzasadnione interesy administratora lub strony trzeciej (np. ochrona mienia lub integralności cielesnej) nie są nadrzędne w stosunku do interesów lub

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

podstawowych praw 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. W rzeczywistości wyważanie interesów ma 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 spółka 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 typu „road blocker". Spółka 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 osób, których dane dotyczą, 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 indywidualnych 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 z osobna (zob. art. 6 ust. 1 lit. f)). Odnoszenie się do abstrakcyjnych sytuacji lub porównywanie podobnych przypadków ma charakter niewystarczający. Administrator musi ocenić ryzyka związane z naruszeniem praw osób, których dane dotyczą; w tym przypadku decydującym kryterium jest intensywność interwencji w odniesieniu do praw i wolności osób fizycznych.

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 charakter i zakres oceny danych.

34. Istotnymi czynnikami równoważącymi mogą być wielkość terenu objętego monitoringiem oraz liczba osób, których dane dotyczą, objętych monitoringiem. Korzystanie z monitoringu wizyjnego w regionie odległym (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 poważnego naruszenia praw osób, których dane dotyczą[11].

35.

3.1.3.2 Uzasadnione oczekiwania osób, których dane dotyczą

36. Zgodnie z motywem 47 stwierdzenie istnienia prawnie uzasadnionego interesu wymaga przeprowadzenia dokładnej oceny. Należy tu uwzględnić uzasadnione oczekiwania osób, których dane dotyczą, w czasie i w kontekście przetwarzania ich danych osobowych. Jeżeli chodzi o systematyczne monitorowanie związku między osobą, której dane dotyczą, a administratorem może znacznie się różnić i wpływać negatywnie na ewentualne uzasadnione oczekiwania osoby, której dane dotyczą. Wykładnia pojęcia „uzasadnione oczekiwania" nie powinna opierać się jedynie na subiektywnych oczekiwaniach. Decydującym kryterium powinno być raczej to, czy obiektywna strona trzecia mogłaby zasadnie oczekiwać, że zostanie objęta monitoringiem w tej konkretnej sytuacji lub wyrazić na to zgodę.

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 zostanie zamontowany w czyimś prywatnym ogrodzie, w strefach zamieszkania lub w gabinetach lekarskich i zabiegowych. Z tego samego względu nie należy oczekiwać, że monitoring zostanie zamontowany w pomieszczeniach sanitarnych lub saunach – monitorowanie takich pomieszczeń stanowi znaczne naruszenie praw osób, których dane dotyczą. Osoby, których dane dotyczą, zasadnie oczekują, że monitoring wizyjny nie zostanie zamontowany w wyżej wymienionych obiektach. 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 powrotowi do zdrowia, rekonwalescencji i wypoczynkowi, a także w miejscach, w których osoby się zatrzymują lub komunikują ze sobą, takich jak przestrzenie z wyznaczonymi miejscami do siedzenia, stoliki w restauracjach, parki, kina i obiekty sportowe. 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 obecności monitoringu wizyjnego nie są istotne przy określaniu ewentualnych obiektywnych oczekiwań osób, których dane dotyczą. Oznacza to, że np. właściciel sklepu nie może powoływać się na obiektywne uzasadnione 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 Konieczność realizacji zadania wykonywanego 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 konieczne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej[13]. Może się okazać, że w ramach wykonywania władzy publicznej nie zezwala się na takie przetwarzanie, lecz inne podstawy prawne, takie jak „zdrowie i bezpieczeństwo" dla ochrony odwiedzających i pracowników mogą zapewniać ograniczony zakres przetwarzania, przy jednoczesnym uwzględnieniu zobowiązań 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 poprzez bardziej precyzyjne określenie szczegółowych wymogów w zakresie przetwarzania, o ile są one zgodne z zasadami ustanowionymi na mocy RODO (np. ograniczenie przechowywania, proporcjonalność).

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

43. Zgoda musi zostać wyrażona dobrowolnie, odnosić się do określonej sytuacji, być świadoma i jednoznaczna, jak określono w wytycznych dotyczących zgody[14].

44. Jeżeli chodzi o systematyczne monitorowanie zgoda osoby, której dane dotyczą, może jedynie służyć jako podstawa prawna, jeżeli jest zgodna z art. 7 (zob. motyw 43) w wyjątkowych przypadkach. Cechą charakterystyczną monitoringu jest to, że technologia ta pozwala na monitorowanie nieograniczonej liczby 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 ewentualna odmowa nie wpłynęła negatywnie na kolegów z drużyny.

45.

46. W przypadku gdy administrator zamierza powołać się na udzieloną zgodę musi zapewnić, aby każda osoba, której dane dotyczą, wchodząca na dany teren objęty monitoringiem wizyjnym, wyraziła zgodę na objęcie monitorowaniem. Zgoda ta musi spełniać warunki określone w art. 7. Wejście na oznaczony teren objęty monitoringiem (np. dane osoby zachęca się do przejścia przez specjalny korytarz lub bramkę, aby mogły wejść na teren objęty monitoringiem) nie stanowi oświadczenia lub jednoznacznej

[13] Podstawę przetwarzania, o którym mowa powyżej, ustanawia prawo Unii lub państwa członkowskiego i jest 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, które są niezbędne do udzielenia zgody, chyba że spełnia kryteria ustanowione w art. 4 i 7, jak określono w wytycznych dotyczących zgody[15].

47. Z uwagi na brak równowagi między prawami pracodawców i pracowników, w większości przypadków, pracodawcy nie powinni powoływać się na zgodę przy przetwarzaniu danych osobowych, ponieważ istnieje małe prawdopodobieństwo, że zostanie ona udzielona dobrowolnie. W tym kontekście należy wziąć pod uwagę wytyczne dotyczące zgody.

48. Państwa członkowskie mogą zawrzeć w swoich przepisach lub porozumieniach zbiorowych, w tym w „umowach o roboty budowlane" szczegółowe przepisy dotyczące przetwarzania danych osobowych pracowników w kontekście zatrudnienia (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 wynikające z RODO.

4.1 Ujawnienie nagrań wideo stronom trzecim – zarys

50. Pojęcie „ujawnienia" zdefiniowano w art. 4 ust. 2 jako przesłanie (np. komunikacja indywidualna), rozpowszechnianie (np. publikowanie w internecie) lub innego rodzaju udostępnianie. Pojęcie „strona trzecia" 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 załadować nagranie do internetu, musi przyjąć podstawę prawną 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, o których mowa w 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 wszczęcia postępowania. 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, zwłaszcza określając podstawę prawną dla przetwarzania swoich danych (np. otrzymywanie materiałów) na podstawie art. 6.

4.2 Ujawnienie nagrań wideo organom ścigania

56. Ujawnienie nagrań wideo organom ścigania jest również niezależnym procesem, w ramach którego wymaga się przedstawienia administratorowi 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 dowodów organom ścigania. Przetwarzanie z upoważnienia administratora przekazującego dane podlega regulacjom na mocy przepisów określonych w RODO. W przypadku gdy przepisy krajowe nakładają na administratora obowiązek współpracy z organami ścigania (np. prowadzenia postępowania przygotowawczego) podstawa prawna dla przekazywania danych stanowi zobowiązanie prawne, o którym mowa w art. 6 ust. 1 lit. c).

58. W takim przypadku zasada celowości, o której mowa w art. 6 ust. 4, zazwyczaj nie stanowi problemu, ponieważ ujawnienie wyraźnie odwołuje się do prawa państwa członkowskiego. W związku z tym nie ma potrzeby uwzględniania specjalnych wymogów w odniesieniu do zmiany celu w kontekście lit. a)–e).

Przykład: Właściciel sklepu prowadzi monitoring obiektu już przy wejściu. 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), (zobowiązanie prawne) w związku z odpowiednimi przepisami krajowymi dotyczącymi przesyłania i przetwarzania.

59.

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 w większości przypadków zostały spełnione warunki, o których mowa w art. 6 ust. 1 lit. f). Ma to zazwyczaj miejsce w sytuacji gdy właściciel sklepu ma uzasadnione podejrzenie, że doszło do popełnienia przestępstwa.

60.

61. Przetwarzanie danych osobowych przez same organy ścigania nie jest zgodne z przepisami RODO (zob. art. 2 ust. 2 lit. d)), lecz jest zgodne z przepisami dyrektywy o ochronie danych (UE2016/680).

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 dane dotyczące szczególnych kategorii danych. Pozornie nieistotne dane zgromadzone za pośrednictwem nagrań wideo mogą być rzeczywiście wykorzystywane do uzyskania innych informacji do różnych celów (np. zobrazowania przyzwyczajeń osób fizycznych). Monitoring wizyjny nie zawsze jest jednak uznawany za przetwarzanie szczególnych kategorii danych osobowych.

> Przykład: Nie uważa się, aby nagranie wideo przedstawiające osobę, której dane dotyczą, w okularach lub na wózku inwalidzkim, dotyczyło samo w sobie szczególnych kategorii danych osobowych.

63.

64. Jeżeli nagranie wideo jest jednak przetwarzane w celu określenia 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: Zamontowanie kamery wideo w szpitalu w celu monitorowania stanu zdrowia pacjenta zostałoby uznane za przetwarzanie szczególnych kategorii danych osobowych (art. 9).

65.

66. Co do zasady, w przypadku każdorazowego instalowania systemu monitoringu wizyjnego, należy dokładnie rozważyć zasadę minimalizacji danych. W związku z tym 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 koniecznością zabezpieczenia żywotnych interesów osoby i udowodnić, że to "[…] 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. A konkretnie, administratorzy danych przetwarzający te dane w kontekście monitoringu wizyjnego nie mogą powoływać się na art. 9 ust. 2 lit. e), w którym zezwala się na przetwarzanie danych osobowych, które są w sposób oczywisty ujawniane publicznie przez osobę, której dane dotyczą. Sam fakt przebywania w miejscu objętym monitoringiem nie oznacza, że osoba, której dane dotyczą, zamierza podać do wiadomości publicznej szczególne kategorie danych, które jej dotyczą.

71. Ponadto przetwarzanie szczególnych kategorii danych wymaga wzmożonej i nieustannej czujności w odniesieniu do pewnych zobowiązań; na przykład wysokiego poziomu bezpieczeństwa i oceny skutków dla ochrony danych, w stosownych przypadkach.

> 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 funkcji rozpoznawania twarzy, wiąże się ze zwiększonymi ryzykami dla praw osób, których dane dotyczą. Pierwszorzędne znaczenie ma wykorzystanie takich technologii z należytym uwzględnieniem zasad legalności, konieczności, proporcjonalności i minimalizacji danych, jak określono w RODO. Wykorzystanie 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 zgodnego z prawem celu przetwarzania.

74. Aby dane zostały zakwalifikowane jako dane biometryczne, jak określono w RODO, przetwarzanie surowych danych, takich jak cechy fizyczne, fizjologiczne lub behawioralne osoby fizycznej, musi określać sposób pomiaru tych cech charakterystycznych. 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 utrwalające wizerunek 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,

[16] Motyw 51 RODO jest dowodem na poparcie tej analizy 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. […]".

- **Środki i sposób przetwarzania**: dane, które „wynikają ze specjalnego przetwarzania technicznego”,

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

77. Wykorzystywanie monitoringu wizyjnego, w tym biometrii, zamontowanego przez podmioty prywatne w celach osobistych (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)), zastosowanie może mieć jednak 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 ATIS w celu stworzenia i zarejestrowania wizerunku twarzy przypisanego do ich karty pokładowej i dowodu tożsamości. Punkty kontroli z funkcją rozpoznawania twarzy muszą być wyraźnie oddzielone, tzn. system należy zainstalować na terenie rękawa lotniczego, aby szablony biometryczne osoby, która nie wyraża zgody, nie zostały zarejestrowane. Tylko pasażerowie, którzy uprzednio wyrazili zgodę i kontynuowali rejestrację, skorzystają z rękawa lotniczego wyposażonego 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 po wciśnięciu 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 zapewniają, 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 teren lub wejścia na inny teren (np. w celu dalszego projektowania spersonalizowanych reklam), wówczas celem będzie jednoznaczne zidentyfikowanie osoby fizycznej, co oznacza że od samego początku procedura ta wchodziłaby w zakres art. 9. Taka sytuacja miałaby miejsce w przypadku gdy administrator przechowuje wygenerowane szablony w celu dalszego umieszczania spersonalizowanych reklam na różnych bilbordach w różnych zakątkach sklepu. Z uwagi na to, że system wykorzystuje cechy fizyczne do wykrywania konkretnych osób fizycznych ponownie wchodzących na teren objęty monitoringiem (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 zostanie 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 na terenie objętym monitoringiem, 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 fizyczne, które chce rozpoznać na podstawie bazy danych od tych, które nie zostały zarejestrowane. Z uwagi na to, że celem jest jednoznaczne zidentyfikowanie osób fizycznych, nadal istnieje potrzeba wprowadzenia wyjątku, określonego w art. 9 ust. 2 RODO, 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 w przypadku udziału osoby, która wyraziła zgodę.

Przykład: Hotel korzysta z monitoringu wizyjnego w celu automatycznego powiadomienia menadżera hotelu o przybyciu ważnej osobistości (*ang. VIP*) zaraz po tym jak wizerunek takiej osoby zostanie rozpoznany. 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 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, m.in. zeskanować bilet). Wejścia wyposażone w urządzenia biometryczne muszą zostać zamontowane 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 uzależnia udzielenia dostępu do swoich usług od wyrażenia zgody na przetwarzanie biometryczne. 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 mierzą się z ograniczeniami urządzenia biometrycznego (niemożność rejestracji lub odczytu danych biometrycznych, trudności z korzystaniem z urządzenia ze względu na niepełnosprawność itd.) oraz w sytuacji, gdy przewiduje się, że korzystanie z urządzenia biometrycznego nie będzie możliwe (np. ze względu na nieprawidłowe działanie), należy przyjąć rozwiązanie alternatywne, aby zapewnić ciągłość zaproponowanych usług, które podlegają jednak ograniczeniom i są dostępne w wyjątkowych okolicznościach. W wyjątkowych przypadkach przetwarzanie biometryczne stanowi główną działalność w ramach usług przewidzianych umową, np. muzeum, które organizuje wystawę, aby zaprezentować wykorzystanie urządzenia do rozpoznawania twarzy, w którym to przypadku osoby, których dane dotyczą, nie będą mogły wnieść sprzeciwu wobec 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 na podstawie wizerunku cyfrowego niezbędne do 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 były 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 do 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 – przechowywane 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 udzieleniu 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 zgłębić wiedzę na temat metod addytywnych (takich jak dodawanie znaku wodnego), które skutkowałyby nieskutecznym tworzeniem szablonów. 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 DOTYCZĄ DANE

91. Z uwagi na charakter przetwarzania danych przy korzystaniu z monitoringu wizyjnego, niektóre prawa osób, których dane dotyczą, przewidziane w RODO służą dalszemu wyjaśnieniu. 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 będą przetwarzane, czy też nie. W przypadku monitoringu wizyjnego oznacza to, że jeżeli nie przechowuje ani nie przesyła się żadnych danych, wówczas czas, w którym miało mieć miejsce monitorowanie w czasie rzeczywistym, upłynął, a administrator mógł 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 nieustannie 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 negatywnie wpływa na prawa innych osób

94. Z uwagi na fakt, że w tej samej sekwencji monitoringu wizyjnego można zarejestrować nieograniczoną liczbę osób, których dane dotyczą, monitorowanie mogłoby wówczas 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 negatywnie 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, jeżeli można na nich zidentyfikować inne osoby, których dane dotyczą. Ochrona praw stron trzecich nie powinna jednak służyć za wymówkę dla uniemożliwiania zgodnego z prawem dostępu osobom fizycznym. W takich przypadkach administrator powinien wdrożyć środki techniczne w celu realizacji żądania w sprawie 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 wyszukać nagrania wideo w celu uzyskania 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 swojego wizerunku za pomocą dokumentu tożsamości lub osobiście) we wniosku skierowanym do administratora sprecyzować, kiedy – w rozsądnym terminie proporcjonalnie do ilości zarejestrowanych osób, których dane dotyczą – wszedł na teren 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 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 na przykład administrator automatycznie usuwa wszystkie nagrania w ciągu dwóch dni, administrator nie jest 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 początkowo zgromadzone lub, w przypadku gdy przetwarzanie jest niezgodne z prawem (zob. również Sekcja 8 – okres przechowywania danych i obowiązek usunięcia danych). Ponadto w zależności od podstawy prawnej przetwarzania dane osobowe powinny zostać usunięte:

- *ze względu na zgodę*, w przypadku wycofania zgody (nie istnieje żadna inna podstawa prawna przetwarzania),
- *ze względu na prawnie uzasadniony interes.*

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

101. W przypadku udostępnienia nagrania wideo przez administratora (np. publikowania lub transmisji strumieniowej na żywo) należy podjąć uzasadnione kroki w celu poinformowania innych administratorów (którzy obecnie przetwarzają dane osobowe) o wniesionym żądaniu 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. *Sekcja 8*).

103. W przypadku monitoringu wizyjnego należy zauważyć, że, na przykład zamazywanie 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 w przechowywaniu danych, który miałyby 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, na podstawie szczególnej sytuacji, w której się znajduje, wobec przetwarzania zgodnie z art. 21 RODO. Przetwarzanie danych osoby fizycznej musi zostać wstrzymane, chyba że administrator wykaże ważne i uzasadnione powody, które mają charakter nadrzędny 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 teren objęty monitoringiem, w trakcie lub po zakończeniu tego procesu. W praktyce oznacza to, że, o ile administrator nie ma ważnych i uzasadnionych powodów, monitorowanie danego terenu, na którym możliwe byłoby zidentyfikowanie osób fizycznych, jest zgodne z prawem jedynie wówczas gdy

(1) administrator może niezwłocznie zapobiec przetwarzaniu 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 teren, do którego osoba, której dane dotyczą, nie ma dostępu jako obywatel.

107. Niniejsze wytyczne nie służą określeniu czym jest *ważny* i 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 naruszenia 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 ze względu na szczególną sytuację, w której się znajduje. 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 i uzasadnione powody, aby kontynuować przetwarzanie danych osobowych.

109.

7 PRZEJRZYSTOŚĆ I OBOWIĄZKI INFORMACYJNE[18]

110. Już od dawna nieodłącznym elementem europejskiego prawa o ochronie danych była świadomość osób, których dane dotyczą, na temat funkcjonowania monitoringu wizyjnego. Osoby te należy poinformować w sposób szczegółowy 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 WP260 pkt 26 art. 13 RODO ma zastosowanie, w przypadku gdy dane osobowe pozyskiwane są „[...] od osoby, której one dotyczą, poprzez obserwację (np. wykorzystując urządzenia zautomatyzowanego przechwytywania danych lub oprogramowania do przechwytywania danych, takich jak kamery [...]".

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

7.1 Informacje zawarte w pierwszej warstwie (znak ostrzegawczy)

112. Pierwsza warstwa przekazuje informacje na temat podstawowego sposobu, w jaki administrator po raz pierwszy kontaktuje się 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 teren 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 został uchwycony 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. szczegółowe dane na temat 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

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

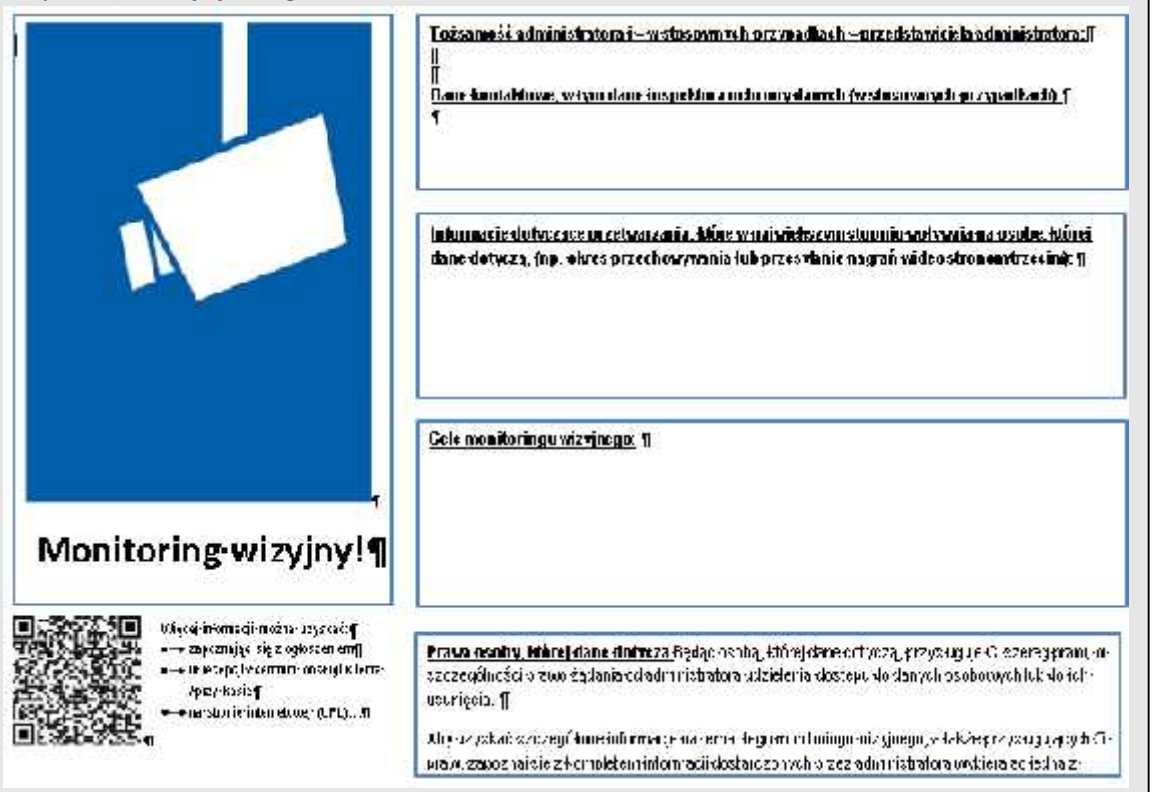
[19] Zob. WP859, Opinia 4/2004 w sprawie przetwarzania danych osobowych przy nadzorze z użyciem kamer video (Grupa Robocza Art. 29).

[20] Zob. WP260, pkt 38.

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

115. Ponadto znak powinien zawierać wszelkie informacje, które mogłyby stanowić zaskoczenie dla osoby, której dane dotyczą (WP260, pkt 38). Sytuacje takie obejmują na przykład przekazywanie danych stronom trzecim, zwłaszcza jeżeli przebywają one 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 nagrywania danych lub przekazywania danych stronom trzecim).

Przykład (niewiążąca sugestia):



116.

7.2 Informacje zawarte w drugiej warstwie

117. Informacje zawarte w drugiej warstwie 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, recepcji lub przy kasie) lub przedstawić na łatwo dostępnym plakacie. Jak wspomniano powyżej pierwsza warstwa – znak ostrzegawczy – musi wyraźnie odnosić się do informacji zawartych w drugiej warstwie. 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 teren objęty monitoringiem, zwłaszcza jeżeli informacje zostały udostępnione w formie cyfrowej (można to osiągnąć wchodząc na odpowiednią stronę internetową). Inne odpowiednie środki obejmują, m.in. numer telefonu, na który można dzwonić. Bez względu na sposób dostarczenia informacji, muszą one zawierać wszelkie obligatoryjne 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. Mogę one obejmować na przykład: kamery do geolokalizacji oraz zawieranie informacji w aplikacjach mapowych lub na stronach internetowych, aby osoby fizyczne mogły z łatwością, z jednej strony, zidentyfikować i określić źródła wideo dotyczące wykonywania 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 umieścić znak ostrzegawczy w łatwo widocznym miejscu przy wejściu do sklepu, który zawiera informacje pierwszej warstwy. Ponadto musi on dostarczyć arkusz informacyjny zawierający informacje drugiej warstwy przy kasie lub w innym łatwo widocznym i dostępnym miejscu w sklepie.

119.

8 OKRESY PRZECHOWYWANIA I OBOWIĄZEK USUNIĘCIA DANYCH

120. Danych osobowych nie można przechowywać przez czas dłuższy niż to konieczne do celów, dla których dane 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. Bez względu na to, czy istnieje konieczność przechowywania danych, czy też nie, powinny one podlegać kontroli w ograniczonym terminie. Co do zasady prawnie uzasadnione cele prowadzenia monitoringu wizyjnego często służą ochronie mienia lub zabezpieczeniu dowodów. 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 ustaleń organizacyjnych z wyprzedzeniem (np. wyznaczenie, w stosownych przypadkach, przedstawiciela ds. monitorowania i zabezpieczenia 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. w 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 konieczne 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 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, utraty, zmiany, nieuprawnionego ujawnienia lub dostępu do danych pochodzących z monitoringu wizyjnego. Zgodnie z art. 24 i 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 strategie polityczne, 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 elementy zostały pogrupowane w następujące kategorie:

- Środowisko wizualne: utrwalanie wizerunku, wzajemne połączenia i przetwarzanie obrazów;
  - celem utrwalania wizerunku 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. łącze 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 systemu, SMW posiada następujące funkcje logiczne:
  - zarządzanie danymi i zarządzanie działaniami, które obejmują polecenia operatora przetwarzającego oraz działania generowane przez system (procedury uruchomienia alarmu, podmioty alarmujące),
  - interfejsy innych systemów mogą obejmować połączenia z innymi systemami zabezpieczeń (kontrola dostępu, alarm pożarowy) oraz systemami bez zabezpieczeń (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 wiąże się z zapobieganiem utracie lub manipulacji danych.

[21] RODO nie zawiera żadnej definicji, techniczny opis można zaleźć, na przykład w EN 62676-1-1:2014 Systemy monitoringu wizyjnego do zastosowania w aplikacjach dotyczących bezpieczeństwa – część 1–1: Wymogi dotyczące systemu wideo.

125.

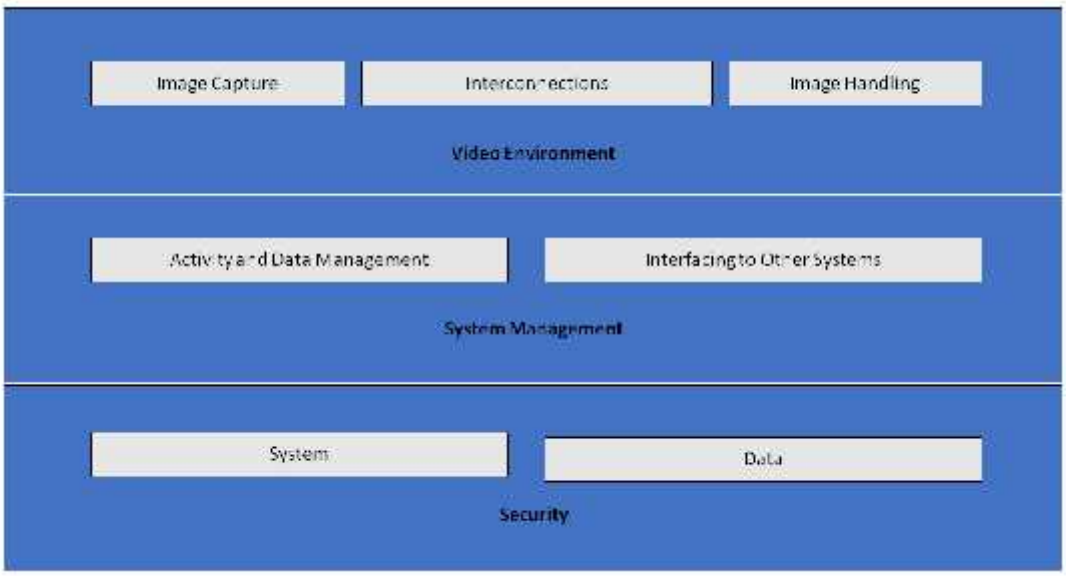


Image Capture	Utrwalanie wizerunku
Interconnections	Wzajemne połączenia
Image Handling	Przetwarzanie obrazów
Video Environment	Środowisko wizualne
Activity and Data Management	Zarządzanie działaniami i danymi
Interfacing to Other Systems	Połączenia z innymi systemami
System Management	Zarządzanie systemem
System	Układ
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 konieczność stworzenia 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 strategie polityczne 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, zasada celowości, domyślna minimalizacja danych w rozumieniu art. 25 ust. 2 RODO, integralność i poufność

[22] WP 168, Opinia 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.).

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 zapewnić odpowiednią ochronę wszystkich elementów składowych systemu monitoringu wizyjnego i danych na wszystkich etapach, tj. w trakcie przechowywania (dane odłożone), przesyłania (dane przesyłane) i przetwarzania (dane wykorzystywane). W tym celu administratorzy i podmioty przetwarzające muszą zastosować strategię łączącą 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, dostarczając nagrania wideo osobom, których dane dotyczą[23]. Z drugiej strony wybrane rozwiązania nie powinny zawierać funkcji, które nie są niezbędne (np. nieograniczone śledzenie ruchów kamery, możliwość przybliżenia, transmisja radiowa, analiza i nagrania dźwiękowe). Funkcje, które nie są niezbędne, należy dezaktywować.

130. Istnieje wiele materiałów na ten temat, w tym informacje na temat norm międzynarodowych i specyfikacji technicznej 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. Sekcja 10) administratorzy powinni wziąć pod uwagę następujące tematy przy tworzeniu swoich strategii politycznych i procedur w zakresie monitoringu wizyjnego:

- Kto odpowiada za zarządzanie i obsługę systemu monitoringu wizyjnego.
- Cel i zakres projektu poświęconego monitoringowi wizyjnemu.
- Właściwe i niedozwolone wykorzystanie (w jakich miejscach i w jakim czasie wykorzystanie monitoringu wizyjnego jest dozwolone; 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 – Zabezpieczenia multimedialne – Wytyczne 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 Sekcji 7 (Przejrzystość i obowiązki informacyjne).
- W jaki sposób rejestruje się nagrania wideo i na jaki czas, uwzględniając okres archiwizacji nagrań wideo dotyczący incydentów związanych z bezpieczeństwem informacji.
- Kto musi przejść odpowiednie szkolenie i kiedy.
- Kto ma dostęp do nagrań wideo i w jakich celach.
- Procedury operacyjne (np. kto i gdzie sprawuje nadzór nad monitoringiem wizyjnym, jak postępować w przypadku naruszenia ochrony danych).
- Jakie procedury wnioskowania o uzyskanie dostępu do nagrań wideo muszą stosować strony zewnętrzne, a jakie procedury w przypadku odrzucenia lub uznania wniosku.
- Procedury dotyczące zamówienia, instalacji i konserwacji SMW.
- Procedury zarządzania przypadkami naruszeń danych 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** (dostęp do danych mają wyłącznie osoby, którym udzielono takiego dostępu), **integralność** (zapobieganie utracie lub manipulowaniu danych) oraz **dostępność** (dostęp do danych jest możliwy po złożeniu wniosku o jego udzielenie).

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 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 mogły je zobaczyć jedynie upoważnieni operatorzy.

- Określono i wdrożono procedury w zakresie udzielenia, zmiany i wycofania dostępu fizycznego i logicznego.
- Wdrożono metody i środki uwierzytelniania i autoryzacji użytkowników, obejmujące m.in. długość haseł i zmianę częstotliwości.
- 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 problemy 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 rodzaj przetwarzanych danych może stanowić wysokie ryzyko dla praw i 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 procesów 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 (tj. ochrona osób i mienia, wykrywanie przestępstw, zapobieganiem im oraz ich kontrola, gromadzenie dowodów 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 wówczas ją przeprowadzić. Wybór administratora w zakresie wdrażanych środków służących ochronie danych powinien być podyktowany wynikiem przeprowadzonej oceny skutków dla ochrony danych.

138. Należy również zauważyć, że wyniki oceny skutków dla ochrony danych wskazują, że przetwarzanie stanowiłoby wysokie ryzyko pomimo planowanego przez administratora wdrożenia środków bezpieczeństwa, a wówczas konieczne będzie skonsultowanie się z odpowiednim organem nadzorczym przed rozpoczęciem przetwarzania. Informacje szczegółowe dotyczące poprzednich 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 (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679. – zatwierdzone przez EROD