Monitoring wizyjny – lista kontrolna

CO WERYFIKUJEMY?	UZASADNIENIE
Czy stosowany jest monitoring w czasie rzeczywistym bez dokonywania zapisu? Czy zapis z monitoringu można przeszukiwać według określonych kryteriów (np. czasu, miejsca)?	Jeśli nadzór prowadzony jest w czasie rzeczywistym bez dokonywania zapisu, nie mamy możliwości „powrotu" do nagranych obrazów. Nie powstanie zatem zbiór danych, w ramach którego możliwe byłoby odszukanie danych określonej osoby. Dla zakwalifikowania nagrań jako zbioru danych istotne jest to, czy jest to zestaw informacji dostępny według określonych kryteriów.
Czy zapisywany jest wyłącznie obraz czy również głos?	Nagrywanie głosu musi być legalne. Konieczne jest zatem wykazanie podstawy prawnej takiego działania. W przypadku nagrywania obrazu, będą to zazwyczaj względy bezpieczeństwa (art. 23 ust. 1 pkt 5 UODO).
Czy obraz z kamer umożliwia zidentyfikowanie osób?	Analizy wymaga to, czy obraz utrwalany za pomocą systemu monitoringu spełnia kryteria pojęcia „danych osobowych".
Jaki rodzaj danych przetwarzany jest przy użyciu monitoringu (dane zwykłe/dane wrażliwe)?	Rodzaj danych wpływa m.in. na podstawę prawną ich przetwarzania (art. 23 ust. 1 UODO – dane zwykłe, art. 27 ust. 2 UODO – dane wrażliwe).
Jaki zakres danych przetwarzany jest przez system monitoringu? Czy zapis z monitoringu można powiązać z innymi informacjami posiadanymi przez dany podmiot (np. księgą wejść, przepustkami, identyfikatorami)?	Ustalenie zakresu przetwarzanych danych jest istotne m.in. z punktu widzenia: — opisu struktury zbiorów danych w Polityce bezpieczeństwa, — wypełniania zgłoszenie zbioru danych do rejestracji GIODO, — realizacji zasady adekwatności wyrażonej w art. 26 ust. 1 pkt 3 UODO.

KANCELARIA LEX ARTIST
UL. SZANCOWA 74/1
01-458 WARSZAWA
TELEFON: (22) 253 28 18
E-MAIL: KANCELARIA@LEX-ARTIST.PL

REGON: 141235395
NIP: 522-267-65-39
BRE BANK S.A. 62 1140 2004 0000 3602 5030 0372

Rozmieszczenie kamer: — na zewnątrz? — wewnątrz budynku? (korytarze, pomieszczenia biurowe, pomieszczenia socjalne – np. stołówki)	Weryfikacja rozmieszczenia kamer i obszaru objętego ich zasięgiem pozwoli na zminimalizowanie ryzyka naruszenia prywatności pracowników, klientów i innych osób przebywających w obszarze monitorowanym.
Na jakim nośniku zapisywane są nagrania?	Informację tę warto uwzględnić w Instrukcji zarządzania systemem informatycznym (określenie sposobu, okresu i miejsca przechowywania elektronicznych nośników informacji zawierających dane osobowe).
Jak długo przechowywane są nagrania?	Okres przechowywania nagrań jest istotny z punktu widzenia zasady ograniczenia czasowego, wyrażonej w art. 26 ust. 1 pkt 4 UODO. Zazwyczaj nagrania przechowywane są przez 7-14 dni.
Gdzie przechowywane są nagrania?	Miejsce przechowywania nagrań będzie stanowiło obszar przetwarzania danych, który wskazujemy w Polityce bezpieczeństwa.
W jaki sposób nagrania są usuwane?	Odpowiedź na to pytanie pozwoli m.in. na ustalenie, kto uzyskuje dostęp do nagrań. Ponadto, w przypadku gdy nośniki przekazywane są celem zniszczenia podmiotowi zewnętrznemu, będziemy mieli do czynienia z powierzeniem przetwarzania danych. Dodatkowo, jeśli nagrania są nadpisywane, okres rotacji będzie wyznaczał czas przechowywania poszczególnych nagrań.
Kto i na jakich zasadach może uzyskać dostęp do nagrań?	W celu zapewnienia ochrony danych przed ich udostępnieniem osobom nieupoważnionym, warto opracować zasady dostępu do nagrań.
System służący do monitorowania: — nazwa, — czy jest to system własny czy dostarcza go podmiot zewnętrzny? — czy podmioty zewnętrzne uzyskują stały dostęp do nagrań (np. ochrona, IT)? — czy system spełniania wymogi Rozporządzenia?	Informacje te uwzględniamy w Polityce bezpieczeństwa i Instrukcji zarządzania systemem informatycznym. Dodatkowo, weryfikujemy spełnianie wymogów Rozporządzenia (w szczególności § 7) i to, czy dane są powierzane.

Czy uwzględniono zbiór w dokumentacji ochrony danych osobowych: — Polityka Bezpieczeństwa, — Instrukcja zarządzania systemem informatycznym, — upoważnienia do przetwarzania danych osobowych, — ewidencja osób upoważnionych, — umowy powierzenia przetwarzania danych osobowych.	Wyodrębnienie zbioru musimy uwzględnić w Polityce bezpieczeństwa i Instrukcji zarządzania systemem informatycznym. Osobom mającym dostęp do danych należy wydać upoważnienia, które następnie wymagają zaewidencjonowania. Ponadto, jeśli podmioty zewnętrzne uzyskują dostęp do nagrań (np. podmiot świadczący usługę obsługi i serwisu sprzętu monitorującego), musimy – zgodnie z art. 31 UODO – zawrzeć pisemne umowy powierzenia.
Czy znajduje zastosowanie zwolnienie z obowiązku rejestracyjnego (art. 43 ust. 1 i 1a UODO)?	Jeśli nie można powołać się na żadne ze zwolnień z obowiązku rejestracyjnego, konieczne jest zgłoszenia zbioru do rejestracji.
Jeśli powołano ABI – czy zbiór podlega uwzględnieniu w jawnym rejestrze prowadzonym przez ABI?	W przypadku, gdy dany podmiot powołał ABIego, osoba ta musi sprawdzić, czy zbiór ten podlega ujawnieniu w jawnym rejestrze (art. 36a ust. 2 pkt 2 UODO).
W jaki sposób realizowany jest obowiązek informacyjny?	Powinniśmy zweryfikować, czy obszar objęty monitoringiem jest właściwie oznaczony (piktogramy, tablice), czy pracownicy (np. poprzez regulamin pracy) informowani są o monitoringu, czy przekazujemy informacje, o których mowa w art. 24 UODO.