Załącznik IX

Instrukcja zarządzania systemem monitoringu wizyjnego

§ 1
Postanowienia ogólne

Instrukcja zarządzania systemem monitoringu, zwana dalej „Instrukcją", opracowana została jako dokument określający zasady i procedury związane z zarządzaniem systemem monitoringu wizyjnego, wprowadzonego w związku z koniecznością zapewnienia bezpieczeństwa wewnętrznego osób i mienia Jednostki, osób przez nią zatrudnionych oraz Pacjentów.

§ 2
Definicje

- **Administrator danych** – "Medar" Sp. z o.o. z siedzibą w Częstochowie ul.Wieluńska 28 reprezentowana przez Zarząd
- **Administratorze systemu monitoringu** – osoba odpowiedzialna za wdrożenie niniejszej Instrukcji oraz jej stosowanie.
- **Użytkownik** – użytkownik z podstawowymi uprawnieniami, jedynie do wglądu w obraz z kamer, do podglądu obrazu.
- **Operator** – osoba z uprawnieniami użytkownika rozszerzonymi o do bezpośredniego dostępu i przetwarzania danych osobowych zarejestrowanych przez system jeśli dysponuje system taką funkcjonalnością.
- **Monitoring** – odbiór obrazu w przestrzeni znajdującej się w polu widzenia kamer monitorowanego obszaru.
- **System monitoringu** – zespół kamer, urządzeń przesyłowych, urządzeń odtwarzających albo rejestrująco/odtwarzających, elektronicznych nośników danych oraz oprogramowania wykorzystywanego w celu osiągnięcia określonej funkcjonalności w zakresie monitoringu.
- **Obszar monitoringu** – przestrzeń znajdująca się w polu widzenia kamer monitorowanego obszaru. Szczegółowy obszar monitoringu opisany jest w Załączniku nr 1 do niniejszej Instrukcji
- **Przetwarzanie danych** – działanie polegające na przeglądaniu podglądu albo zarejestrowanego obrazu w celu identyfikacji tożsamości osoby objętej monitoringiem wizyjnym w zależności od zastosowanej funkcjonalności.
- **Incydent** – zdarzenie wymagające przetwarzania danych w celu udokumentowania okoliczności jego wystąpienia.
- **Rejestr Incydentów** – rejestr zawierający datę, czas i dane przetwarzania (dane Użytkownika i jego czynności) oraz zwięzły opis samego Incydentu. Wzór Rejestru Incydentów stanowi Załącznik nr 2 do niniejszej Instrukcji.
- **Podmiot uprawniony** – podmioty, które mogą uczestniczyć w trakcie przetwarzania obrazu oraz uzyskać kopię zarejestrowanego obrazu. Są to Policja, Straż Graniczna, Biuro Ochrony Rządu, Agencja Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne, Żandarmeria Wojskowa, Służba Kontrwywiadu Wojskowego oraz straże gminna/miejska. Wzór ewidencji udostępniania danych z monitoringu stanowi Załącznik nr 3 do niniejszej Instrukcji.
- **Klauzula informacyjna –** Załącznik nr 5 określa wzór klauzuli informacyjnej koniecznej do umieszczenia w obiektach objętych obszarem monitoringu.

§ 3
Zakres i cel Instrukcji

- Celem Instrukcji jest określenie podstawowych zasad właściwego zarządzania systemem monitoringu w zakresie technicznym i organizacyjnym.
- Instrukcję stosuje się do danych przetwarzanych w systemie monitoringu oraz sposobach ich zabezpieczenia.
- Instrukcja zawiera listę obowiązków Użytkownika i Administratora służących ochronie danych osobowych oraz elementów zarządzania systemem monitoringu.
- Jeśli system monitoringu nie przewiduje funkcjonalności w zakresie rejestracji obrazu, odpowiednio

zapisy Instrukcji dotyczące tego aspektu nie znajdują zastosowania i podelgają modyfikacji.

§ 4

Zabezpieczenie danych osobowych w systemie monitoringu

- Zabezpieczenia systemu monitoringu mają służyć zapewnieniu bezpieczeństwa przetwarzanych danych.
- Zabezpieczenia powinny:
  - uniemożliwić dostęp do systemu osobą postronnym,
  - zapewnić przetwarzanie danych wyłącznie Użytkownikom,
  - odnotowywać każdą ingerencję Użytkownika w dostępie do danych.
- Infrastruktura techniczna systemu monitoringu powinna być dostępna wyłącznie dla osób uprawnionych, posiadających upoważnienie dopuszczające przetwarzanie danych osobowych.
- Zabezpieczenia przetwarzania danych w systemie monitoringu realizowane są w trzech obszarach: zabezpieczenia systemu, ochrona sprzętu oraz ochrona pomieszczeń.

§ 5

Metody i środki uwierzytelniania Użytkowników

- Użytkownik z uprawnieniami operatora posiada unikalny dla niego identyfikator i stosuje znane wyłącznie jemu hasło.
- W przypadku użytkowników z podstawowymi uprawnieniami dopuszczalne jest utworzenie jednego konta dla grupy osób w celu podglądu obrazu na żywo z ekranu monitora lub poprzez rejestrator.
- W wypadku, gdy z przyczyn technicznych, zastosowanie powyższego standardu nie jest możliwe stosuje najmocniejsze, dostępne zabezpieczenie.

§ 6

Obowiązki Użytkownika z rozszerzonymi uprawnieniami systemu monitoringu

- Użytkownik może przetwarzać dane systemu monitoringu wyłącznie w celu ustalenia szczegółów Incydentu.
- Użytkownik może wykonać kopię danych z systemu monitoringu wyłącznie na polecenie Administratora danych.
- Za zgodą Inspektora Ochrony Danych w przetwarzaniu danych przez Użytkownika może uczestniczyć osoba przyjmująca kopię.
- Użytkownik zobowiązany jest do ochrony danych przed ich przetwarzaniem przez osoby nieuprawnione.
- Użytkownik systemu monitoringu zobowiązany jest do poinformowania Administratora Danych Osobowych o każdym naruszeniu zasad bezpieczeństwa.
- Ewidencję osób upoważnionych do przetwarzania danych w systemie monitoringu prowadzi Administrator danych wg wzoru z Załącznika nr 4 do niniejszej Instrukcji.

§ 8

Obowiązki Administratora Systemu Monitoringu

- Obowiązkiem Administratora Systemu Monitoringu jest zapewnienie bezpieczeństwa danych przetwarzanych w systemie monitoringu.
- Administrator Systemu Monitoringu odpowiada za funkcjonowanie systemu monitoringu, a w szczególności za stosowany w nim sprzęt i oprogramowanie.
- Do obowiązków Administratora Systemu Monitoringu należy:
  - sprawdzenie i testowanie zabezpieczeń systemu monitoringu,
  - reagowanie na próby naruszenia bądź zagrożenia danych monitoringu,
  - informowanie Administratora Danych Osobowych o każdej sytuacji zagrożenia bezpieczeństwa danych.
- Administrator Systemu Monitoringu powierzyć może zadanie określone w pkt. 3 upoważnionemu Użytkownikowi.

§ 9

Przechowywanie danych z systemu monitoringu

- Dane systemu monitoringu przechowywane są na dyskach twardych o dużej pojemności przystosowanych do pracy ciągłej.
- Z zapisanych danych nie jest tworzona kopia zapasowa.
- Dane są przechowywane przez okres 16 dni, po czym następuje ich nadpisanie.

§ 10

Postanowienia końcowe

- Niniejsza Instrukcja i dokumenty z nią powiązane powinny być aktualizowane wraz ze zmieniającymi się przepisami.
- Użytkownicy zobowiązani są do przestrzegania postanowień zawartych w niniejszej Instrukcji.
- Treść niniejszej Instrukcji podaje się w odpowiednim zakresie do wiadomości celem realizacji obowiązków informacyjnych określonych treścią rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (Dz.Urz. UE L 119, s. 1)