Zgodnie z art. 12 i art. 13 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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, dalej „RODO”, informujemy, że:

## 1. Administrator danych osobowych

Administratorem danych osobowych przetwarzanych za pomocą systemu monitoringu wizyjnego jest Uniwersytet Medyczny im. Karola Marcinkowskiego w Poznaniu, z siedzibą przy ul. Fredry 10, 61-701 Poznań, dalej „Uniwersytet” lub „Administrator”.

## 2. Kontakt z Inspektorem Ochrony Danych

Administrator wyznaczył Inspektora Ochrony Danych, z którym można kontaktować się we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z ich przetwarzaniem: pocztą elektroniczną:

iod@ump.edu.pl;

pisemnie na adres Administratora: ul. Fredry 10, 61-701 Poznań, z dopiskiem „Inspektor Ochrony Danych”.

## 3. Zakres monitoringu i kategorie przetwarzanych danych

Monitoring wizyjny obejmuje wejścia i wyjścia z budynków Uniwersytetu, ciągi komunikacyjne, parkingi, teren bezpośrednio przylegający do budynków Uniwersytetu.

W ramach monitoringu przetwarzane mogą być: wizerunek osoby znajdującej się w obszarze monitorowanym; informacje o miejscu i czasie przebywania w obszarze objętym monitoringiem; sposób poruszania się po tym obszarze; wizerunek przedmiotów pozostających w posiadaniu osoby; numery rejestracyjne pojazdów, jeżeli kamery obejmują parking, bramy wjazdowe lub drogi wewnętrzne; informacje o przebiegu zarejestrowanego zdarzenia.

System monitoringu rejestruje wyłącznie obraz i nie rejestruje dźwięku.

## 4. Cele stosowania monitoringu

Dane osobowe pochodzące z monitoringu wizyjnego są przetwarzane w celu:

a) zapewnienia bezpieczeństwa osób przebywających na terenie Uniwersytetu, w tym pracowników, studentów, doktorantów, uczestników zajęć, współpracowników, kontrahentów i gości;

b) ochrony mienia Uniwersytetu oraz mienia osób przebywających na terenie Uniwersytetu;

c) zapobiegania zdarzeniom zagrażającym życiu, zdrowiu lub bezpieczeństwu osób;

d) zapobiegania kradzieżom, uszkodzeniom mienia, aktom wandalizmu oraz innym zdarzeniom naruszającym bezpieczeństwo lub porządek;

e) ustalania przebiegu zdarzeń oraz zabezpieczenia materiału dowodowego, jeżeli doszło do zdarzenia zagrażającego osobom lub mieniu;

f) ustalania, dochodzenia lub obrony roszczeń związanych ze zdarzeniem zarejestrowanym przez system monitoringu;

g) realizowania obowiązków prawnych Administratora, w szczególności obowiązków dotyczących zapewnienia bezpiecznych i higienicznych warunków pracy oraz ochrony mienia.

## 5. Podstawa prawna przetwarzania

Dane osobowe są przetwarzane:

a) na podstawie art. 6 ust. 1 lit. e RODO, tj. gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego przez Uniwersytet w interesie publicznym lub w ramach sprawowania powierzonej mu władzy publicznej, w związku z wykonywaniem zadań publicznej uczelni;

b) w odniesieniu do monitorowania pracowników, dodatkowo na podstawie art. 22² ustawy z 26 czerwca 1974 r. – Kodeks pracy, jeżeli monitoring jest niezbędny do:

zapewnienia bezpieczeństwa pracowników, ochrony mienia, zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę;

c) na podstawie art. 6 ust. 1 lit. c RODO, jeżeli przetwarzanie określonych nagrań jest niezbędne do wykonania obowiązku prawnego ciążącego na Administratorze, w szczególności obowiązku udostępnienia albo zabezpieczenia nagrania na podstawie przepisów prawa lub żądania uprawnionego organu;

d) na podstawie art. 6 ust. 1 lit. e RODO, w zakresie niezbędnym do ustalenia, dochodzenia lub obrony roszczeń związanych z realizacją zadań publicznych Uniwersytetu albo ochroną powierzonego mu mienia.

## 6. Sposób działania monitoringu

Monitoring działa całodobowo.

Kamery są rozmieszczone w oznaczonych miejscach. Monitoring obejmuje wyłącznie obszary niezbędne do realizacji wskazanych powyżej celów.

Obraz z kamer jest: rejestrowany; zapisywany na przeznaczonych do tego rejestratorach lub serwerach; dostępny wyłącznie dla osób upoważnionych; automatycznie usuwany lub nadpisywany po upływie ustalonego okresu przechowywania, chyba że nagranie zostanie wcześniej zabezpieczone. Monitoring nie jest prowadzony w miejscach, w których jego stosowanie prowadziłoby do nieproporcjonalnego naruszenia prywatności, godności lub innych dóbr osobistych, w szczególności w toaletach, szatniach, pomieszczeniach sanitarnych i innych miejscach objętych szczególną ochroną, z zastrzeżeniem wyjątków wyraźnie dopuszczonych przepisami prawa.

## 7. Okres przechowywania nagrań

Nagrania z monitoringu wizyjnego są przechowywane przez okres nieprzekraczający 14 dni od dnia zarejestrowania obrazu. Po upływie tego okresu nagrania są automatycznie i trwale usuwane albo nadpisywane przez kolejne nagrania, chyba że przed upływem tego terminu:

a) nagranie zostało zabezpieczone jako dowód w postępowaniu prowadzonym na podstawie prawa;

b) Administrator otrzymał informację, że nagranie może stanowić dowód w takim postępowaniu;

c) zabezpieczenie nagrania jest niezbędne do wyjaśnienia konkretnego zdarzenia;

d) zabezpieczenie nagrania jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń.

W takim przypadku odpowiedni fragment nagrania jest przechowywany do czasu zakończenia wyjaśniania zdarzenia, prawomocnego zakończenia właściwego postępowania albo upływu okresu, w którym możliwe jest dochodzenie związanych z nim roszczeń, zależnie od podstawy i celu jego zabezpieczenia.

## 8. Odbiorcy danych

Dostęp do danych pochodzących z monitoringu mogą uzyskać:

a) pracownicy i współpracownicy Uniwersytetu posiadający odpowiednie upoważnienie, wyłącznie w zakresie niezbędnym do wykonywania ich obowiązków;

b) podmioty zapewniające ochronę osób i mienia, jeżeli obsługują monitoring na podstawie właściwej umowy;

c) dostawcy i serwisanci systemów monitoringu, systemów informatycznych, rejestratorów i infrastruktury technicznej, wyłącznie w zakresie niezbędnym do świadczenia usług i na podstawie odpowiednich umów;

d) podmioty świadczące na rzecz Uniwersytetu pomoc prawną, audytową lub ubezpieczeniową, jeżeli dostęp do nagrania jest niezbędny do wyjaśnienia zdarzenia, dochodzenia roszczeń lub obrony przed nimi;

e) organy publiczne, służby i inne podmioty uprawnione do uzyskania nagrania na podstawie przepisów prawa, w szczególności Policja, prokuratura, sądy lub organy kontrolne.

## 9. Przekazywanie danych poza Europejski Obszar Gospodarczy

Dane pochodzące z monitoringu wizyjnego nie są przekazywane do państwa trzeciego ani organizacji międzynarodowej.

## 10. Zautomatyzowane podejmowanie decyzji

Dane pochodzące z monitoringu wizyjnego nie są wykorzystywane do podejmowania decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu, które wywoływałyby wobec osoby skutki prawne lub w podobny sposób istotnie na nią wpływały. Dane nie są wykorzystywane do profilowania.

## 11. Prawa osób objętych monitoringiem

Na zasadach określonych w RODO osobie, której dane dotyczą, przysługuje:

1) prawo dostępu do dotyczących jej danych osobowych, w tym uzyskania informacji, czy jej wizerunek znajduje się na nagraniu;

2) prawo żądania ograniczenia przetwarzania;

3) prawo wniesienia sprzeciwu wobec przetwarzania danych opartego na art. 6 ust. 1 lit. e RODO, z przyczyn związanych ze szczególną sytuacją tej osoby;

4) prawo żądania usunięcia danych, jeżeli zachodzą przesłanki określone w art. 17 RODO;

5) prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

Realizacja prawa dostępu do nagrania może podlegać ograniczeniom wynikającym z praw i wolności innych osób utrwalonych na nagraniu. Osoba występująca z żądaniem powinna, w miarę możliwości, wskazać datę, przybliżoną godzinę, miejsce

zdarzenia i inne informacje umożliwiające odnalezienie właściwego fragmentu nagrania. Jeżeli osoba uzna, że przetwarzanie jej danych osobowych narusza przepisy RODO, ma prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych

## 12. Dobrowolność podania danych

Wejście na obszar objęty monitoringiem wiąże się z możliwością zarejestrowania wizerunku osoby przez system monitoringu. Podanie danych w postaci wizerunku nie jest oparte na zgodzie i nie ma charakteru dobrowolnego w tradycyjnym znaczeniu. Dane są pozyskiwane automatycznie w związku z przebywaniem w oznaczonym obszarze objętym monitoringiem.