

ZARZĄDZENIE NR 379/26
PREZYDENTA MIASTA SZCZECIN
z dnia 10 lipca 2026 r.

**w sprawie wprowadzenia regulaminu funkcjonowania systemu monitoringu wizyjnego miasta
Szczecin**

Na podstawie art. 31 w związku z art. 9a ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2026 r. poz. 662), art. 34 ust. 1 w związku z art. 92 ust. 1 pkt 2 i art. 4b ust. 1 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2025 r. poz. 1684 oraz Dz. U. z 2026 r. poz. 252) oraz art. 6 ust. 1 lit. c i e oraz art. 13 i art. 32 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, s.1, Dz. Urz. UE L 127 z 23.05.2018, s.2, Dz. Urz. UE L 74 z 04.03.2021, s.35) **zarządzam, co następuje:**

§ 1. Wprowadza się Regulamin funkcjonowania systemu monitoringu wizyjnego miasta Szczecin, stanowiący załącznik do zarządzenia.

§ 2. Regulamin, o którym mowa w § 1 określa w szczególności:

- 1) cele funkcjonowania monitoringu;
- 2) zasady funkcjonowania, obsługi i eksploatacji monitoringu, w tym zakres i sposób prowadzenia rejestracji obrazu;
- 3) zasady przechowywania, przetwarzania i udostępniania danych;
- 4) tryb realizacji uprawnień osób, których dane są przetwarzane;
- 5) zasady współpracy z uprawnionymi podmiotami.

§ 3. Zarządzanie systemem monitoringu wizyjnego miasta Szczecin powierza się Wydziałowi Informatyki Urzędu Miasta Szczecin.

§ 4. Nadzór nad realizacją zarządzenia sprawuje Sekretarz Miasta.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

Prezydent Miasta

Piotr Krzystek

Załącznik do zarządzenia nr 379/26

Prezydenta Miasta Szczecin

z dnia 10 lipca 2026 r.

REGULAMIN FUNKCJONOWANIA SYSTEMU MONITORINGU WIZYJNEGO MIASTA SZCZECIN

§ 1. 1. Regulamin funkcjonowania systemu monitoringu wizyjnego miasta Szczecin zwany dalej Regulaminem, określa cele funkcjonowania systemu monitoringu wizyjnego miasta Szczecin zwanego dalej Systemem, zasady funkcjonowania, obsługi i eksploatacji Systemu, w tym zakres i sposób prowadzenia rejestracji obrazu, cele, zakres i zasady przechowywania, przetwarzania i udostępniania danych, w tym danych osobowych, tryb realizacji uprawnień osób, których dane są przetwarzane, a także zasady współpracy z uprawnionymi podmiotami.

2. Celem funkcjonowania Systemu jest zapewnienie porządku publicznego i bezpieczeństwa obywateli oraz ochrony przeciwpożarowej i przeciwpowodziowej.

3. System stanowi kluczowy środek wsparcia systemu bezpieczeństwa mieszkańców oraz osób czasowo przebywających na terenie Gminy Miasto Szczecin. Służy on w szczególności rejestrowaniu przestępstw i wykroczeń, zapobieganiu ich występowania oraz wsparciu działań podmiotów zaangażowanych w neutralizację sytuacji kryzysowych.

4. System rejestruje przestrzeń publiczną i zapisuje dane, w tym wizerunek osób przebywających na obszarze objętym monitoringiem wraz z godziną, datą i miejscem. System nie rejestruje dźwięku w przestrzeni publicznej.

5. Administratorem danych rejestrowanych w Systemie jest Gmina Miasto Szczecin.

6. Informacje dotyczące przetwarzania danych osobowych przez administratora danych, stanowią załącznik nr 1 do Regulaminu i umieszczone są w Biuletynie Informacji Publicznej Urzędu Miasta Szczecin.

§ 2. 1. Centrum Przetwarzania Danych Systemu zlokalizowane jest w serwerowni Szczecińskiego Parku Naukowo Technologicznego spółki z ograniczoną odpowiedzialnością, przy ul. Cyfrowej 2-8 w Szczecinie.

2. Centrum Zarządzania Systemu mieści się w budynku Urzędu Miasta Szczecin, przy Placu Armii Krajowej 1 w Szczecinie.

3. Zadania z zakresu zarządzania Systemem obejmujące administrowanie, organizację, utrzymanie oraz obsługę techniczną realizuje i zapewnia Wydział Informatyki Urzędu Miasta Szczecin.

§ 3. 1. W celu zapewnienia bezpieczeństwa i porządku, nadzorem wizyjnym objęte są miejsca publiczne, w których odbywa się największy przepływ osób oraz miejsca szczególnie narażone na zagrożenia. Lokalizacja kamer będzie każdorazowo konsultowana z instytucjami odpowiedzialnymi za bezpieczeństwo mieszkańców i osób przebywających na terenie Gminy Miasto Szczecin.

2. Wykaz lokalizacji kamer Systemu udostępniany jest w Biuletynie Informacji Publicznej Urzędu Miasta Szczecin.

§ 4. 1. System składa się z kamer obrotowych i stałopozycyjnych oraz infrastruktury sieciowej i serwerowej niezbędnej do funkcjonowania monitoringu. Wszystkie kamery Systemu funkcjonują całodobowo, siedem dni w tygodniu. System rejestruje obrazy cyfrowe bez dźwięku. Jakość obrazu pozwala na zidentyfikowanie osób oraz przedmiotów znajdujących się na obszarze objętym monitoringiem. System umożliwia sterowanie kamerami oraz dokonywane zbliżeń obrazu mając na względzie zapewnienie bezpieczeństwa, z zachowaniem zasad godności osobistej i prawa do prywatności.

2. System nie przetwarza danych biometrycznych, czyli danych szczególnych kategorii w rozumieniu art. 9 ust. 1 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 (ogólne rozporządzenie o ochronie danych), zwanego dalej RODO, w szczególności nie umożliwia automatycznego rozpoznawania osób monitorowanych w oparciu o cechy biometryczne.

§ 5. 1. Nagrania z Systemu są przetwarzane na macierzach dyskowych. W celu ochrony danych osobowych stosuje się środki zabezpieczające takie jak:

- 1) odseparowaną, dedykowaną sieć komputerową;
- 2) uwierzytelnianie użytkowników;
- 3) stosowanie zapór sieciowych - uniemożliwiające utratę, bezprawny dostęp i rozpowszechnienie danych zlokalizowanych w Centrum Przetwarzania Danych Systemu;
- 4) umieszczenie serwerów, na których przechowywane są zarejestrowane nagrania, w zabezpieczonych pomieszczeniach.

2. Dostęp do Systemu mają jedynie wyznaczeni i przeszkoleni pracownicy podmiotów posiadających dostęp do Systemu na podstawie zawartych porozumień o udostępnieniu danych lub umów powierzenia przetwarzania danych, którzy zobowiązani są do przestrzegania ustawień prywatności i praw dostępu.

3. Wszystkie pomieszczenia, w których znajdują się urządzenia Systemu, są zabezpieczone przed dostępem osób nieuprawnionych.

4. Zarejestrowane nagrania z Systemu przechowywane są przez okres 30 dni. Po tym czasie są automatycznie nadpisywane.

§ 6. 1. Na pisemny wniosek organów państwowych lub innych podmiotów uprawnionych na podstawie przepisów prawa (m.in. Policja, sądy, prokuratura, służby specjalne), nagranie z Systemu może zostać:

- 1) zabezpieczone, albo
- 2) zabezpieczone i udostępnione.

2. W przypadku, o którym mowa w ust. 1, udostępnienie pełnego nagrania następuje wyłącznie w zakresie niezbędnym do realizacji ustawowych zadań organów i podmiotów. Udostępnienie nagrania następuje wyłącznie w zakresie niezbędnym do realizacji, zgodnego z prawem, celu wskazanego we wniosku o udostępnienie, z zachowaniem zasady minimalizacji danych.

3. Nagranie udostępnia się drogą elektroniczną, z zastosowaniem środków technicznych i organizacyjnych zapewniających integralność oraz poufność danych, poprzez zapewnienie, na okres nie dłuższy niż 14 dni, dostępu do nagrania. W wyjątkowych sytuacjach, na uzasadnione żądanie uprawnionego, nagranie zostanie udostępnione na nośniku.

4. W przypadku braku podstaw do udostępnienia nagrania, w szczególności gdy udostępnienie mogłoby naruszać prawa i wolności innych osób albo gdy wniosek nie spełnia wymogów określonych w Regulaminie, Administrator odmawia udostępnienia.

5. Odmowa udostępnienia nagrania następuje w formie pisemnej.

6. Kopie nagrań sporządzone w celu ich udostępnienia podlegają zniszczeniu po upływie 30 dni od dnia ich sporządzenia, o ile dalsze ich przechowywanie nie jest wymagane na podstawie przepisów prawa.

§ 7. 1. Prawo uzyskania dostępu do nagrania z Systemu, w ramach realizacji prawa dostępu do danych na podstawie art. 15 ust. 1 RODO, przysługuje osobie fizycznej, której dane (wizerunek) zostały zarejestrowane przez System.

2. W przypadku, o którym mowa w ust. 1, dostęp do nagrania poprzedzony jest techniczną anonimizacją (np. trwałym rozmyciem, maskowaniem lub wycięciem) wizerunków osób trzecich oraz innych danych pozwalających na ich identyfikację (np. numerów rejestracyjnych pojazdów). Powyższy wymóg ma na celu zagwarantowanie, że realizacja prawa dostępu wnioskodawcy nie wpłynie niekorzystnie na prawa i wolności innych osób, zgodnie z art. 15 ust. 4 RODO.

3. Przekazanie dostępu do nagrania następuje na okres nie dłuższy niż 14 dni, drogą elektroniczną, z zastosowaniem środków technicznych i organizacyjnych zapewniających integralność oraz poufność danych. W wyjątkowych sytuacjach, na uzasadnione żądanie uprawnionego, prawo dostępu do nagrania zostanie zrealizowane poprzez przekazanie nagrania na nośniku. Jeżeli przekazanie dostępu do zanonimizowanego nagrania nie będzie możliwe bez poważnego naruszenia praw i wolności innych osób (art. 15 ust. 4 RODO), Administrator zrealizuje prawo dostępu w innej formie, np. poprzez umożliwienie wnioskodawcy osobistego wglądu w nagranie w wyznaczonym pomieszczeniu Urzędu Miasta Szczecin, pod nadzorem uprawnionego pracownika i przy zachowaniu środków ostrożności chroniących dane osób trzecich lub poprzez wydanie pisemnego zaświadczenia opisującego treść nagrania.

4. Administrator odmawia dostępu do danych z Systemu w przypadku, gdy:

- 1) na nagraniu nie utrwalono wizerunku wnioskodawcy lub jakość nagrania uniemożliwia jego jednoznaczną identyfikację;
- 2) wniosek ma charakter ewidentnie nieuzasadniony lub nadmierny w rozumieniu art. 12 ust. 5 RODO;
- 3) zachodzi uzasadnione podejrzenie, że umożliwienie dostępu do nagrania mogłoby stanowić zagrożenie dla bezpieczeństwa publicznego, utrudnić zapobieganie przestępczości lub ingerować w toczące się postępowania prowadzone przez uprawnione organy.

5. Kopie nagrań sporządzone w celu udzielenia dostępu do danych w trybie art. 15 RODO podlegają zniszczeniu niezwłocznie po zrealizowaniu prawa osoby, której dane dotyczą, nie później niż po upływie 30 dni od dnia ich sporządzenia, o ile dalsze ich przechowywanie nie jest wymagane na podstawie przepisów prawa.

§ 8. 1. Nagrania z Systemu mogą być zabezpieczane na pisemny wniosek zawierający dane pozwalające na identyfikację nagrania oraz opis zdarzenia uzasadniającego zabezpieczenie.

2. Zabezpieczenie nagrania nie stanowi podstawy do jego udostępnienia.

3. Zabezpieczone nagranie przechowuje się przez okres niezbędny do realizacji celu zabezpieczenia, nie dłużej jednak niż przez 30 dni od dnia zabezpieczenia. Po upływie terminu, o którym mowa w zdaniu poprzednim, zabezpieczone nagranie podlega usunięciu, o ile jego dalsze przechowywanie nie jest wymagane na podstawie przepisów prawa.

§ 9. Wnioski, o których mowa w §6 ust.1 oraz w §8 ust. 1, powinny zawierać co najmniej:

- 1) imię i nazwisko lub nazwę wnioskodawcy;
- 2) dokładną datę, czas i miejsce (dokładna lokalizacja ze wskazaniem kamer według listy kamer) zdarzenia;
- 3) opis zdarzenia;
- 4) cel odpowiednio udostępnienia albo zabezpieczenia nagrania;
- 5) podstawę prawną udostępnienia nagrania;
- 6) podpis.

§ 10. 1. Z czynności zniszczenia kopii nagrania sporządza się protokół. Wzór protokołu stanowi załącznik nr 2 do Regulaminu.

2. Czynność zniszczenia kopii nagrania przeprowadza komisja powoływana przez Dyrektora Wydziału Informatyki Urzędu Miasta Szczecin, w skład której wchodzi pracownicy tego Wydziału.

§ 11. W Urzędzie Miasta Szczecin, odnośnie nagrań z Systemu, prowadzi się:

- 1) rejestr wniosków o udostępnienie nagrań;
- 2) rejestr wniosków o udzielenie dostępu do danych w trybie art. 15 RODO;
- 3) rejestr wniosków o zabezpieczenie nagrań.

**Informacje dotyczące przetwarzania danych osobowych
OBOWIĄZEK INFORMACYJNY**

Gmina Miasto Szczecin – Urząd Miasta Szczecin

Na podstawie art. 13 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 (ogólne rozporządzenie o ochronie danych, zwane dalej RODO), przekazuję informacje na temat zasad przetwarzania Pani/Pana danych osobowych.

1. Administratorem danych osobowych jest Gmina Miasto Szczecin – Urząd Miasta Szczecin, Pl. Armii Krajowej 1, 70-456 Szczecin, tel. 914245700, e-mail: informatyka@um.szczecin.pl

2. Administrator wyznaczył Inspektora Ochrony Danych z którym można się skontaktować telefonicznie: 91 42 45 702 oraz mailowo: iod@um.szczecin.pl

3. Dane osobowe będą przetwarzane:

–w zakresie wizerunku w związku z funkcjonowaniem systemu monitoringu wizyjnego miasta Szczecin - na podstawie art. 6 ust. 1 lit. e RODO (przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym) w związku z art. 9a ustawy z dnia 8 marca 1990 r. o samorządzie gminnym oraz art. 4b ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym,

–w zakresie danych identyfikacyjnych osoby fizycznej, która występuje z wnioskiem o dostęp do swoich danych - na podstawie art. 6 ust. 1 lit. c RODO (przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze) w związku z art. 15 RODO.

4. Przetwarzanie wizerunku wynika z przepisów prawa i jest realizowane w interesie publicznym.

5. Przetwarzanie danych identyfikacyjnych osoby fizycznej jest niezbędne do realizacji prawa dostępu do danych w trybie art. 15 RODO.

6. Odbiorcami danych osobowych w zakresie wizerunku zarejestrowanego przez system monitoringu wizyjnego miasta Szczecin będą podmioty świadczące usługi IT na podstawie umów powierzenia przetwarzania danych, w tym Szczeciński Park Naukowo-Technologiczny Sp. z o.o. Odbiorcami mogą być również jednostki, którym przepisy prawa przyznają prawo do przetwarzania danych z systemu monitoringu wizyjnego miasta Szczecin i z którymi Administrator zawarł porozumienia dotyczące udostępniania danych z systemu monitoringu wizyjnego miasta Szczecin tj.: Komendant Wojewódzkiej Policji w Szczecinie, Komendant Miejskiej Policji w Szczecinie, Straż Miejska w Szczecinie, Zarząd Dróg i Transportu Miejskiego w Szczecinie, a także jednostki realizujące zadania publiczne na polecenie administratora: Wodne Ochotnicze Pogotowie Ratunkowe w Szczecinie, Żegluga Szczecińska Turystyka i Wydarzenia Sp. z o.o.

7. Odbiorcami danych identyfikacyjnych osoby fizycznej, która występuje z wnioskiem o dostęp do danych w trybie art. 15 RODO będą podmioty świadczące usługi IT na podstawie umów powierzenia przetwarzania danych.

8. Dane mogą być udostępniane organom publicznym uprawnionym na podstawie przepisów prawa, w ramach prowadzonych przez te organy postępowań.

9. Dane w zakresie wizerunku będą przetwarzane przez okres 30 dni. Nagrania zabezpieczone w związku ze zgłoszonym zdarzeniem przechowywane są przez okres niezbędny do realizacji celu zabezpieczenia, nie dłużej jednak niż 30 dni od dnia ich zabezpieczenia, a po jego upływie podlegają usunięciu, o ile dalsze ich przechowywanie nie jest wymagane na podstawie przepisów prawa.

10. Dane identyfikacyjne osoby fizycznej, która występuje z wnioskiem o dostęp do danych w trybie art. 15 RODO będą przetwarzane do czasu realizacji wniosku, a następnie przechowywane zgodnie z przepisami ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

11. W związku z przetwarzaniem danych przysługują następujące prawa wynikające z przepisów RODO:

- prawo dostępu do danych – art. 15 RODO,
 - prawo do sprostowania danych – art. 16 RODO,
 - prawo do ograniczenia przetwarzania – art. 18 RODO,
- a także

–prawo do sprzeciwu – art. 21 RODO – wyłącznie w przypadku przetwarzania na podstawie art. 6 ust. 1 lit. e RODO.

12. W związku z przetwarzaniem danych przysługuje prawo do wniesienia skargi do organu nadzorczego - Prezesa Urzędu Ochrony Danych Osobowych.

Protokół z czynności zniszczenia nagrań z systemu monitoringu wizyjnego miasta Szczecin

Dnia komisja w składzie:

1.
2.
3.
4.

dokonała trwałego zniszczenia kopii nagrania z Systemu
.....

Dokonanie ww. czynności zostaje potwierdzone podpisami członków komisji:

.....
.....
.....