POLITYKA BEZPIECZEŃSTWA INFORMACJI W ZAKRESIE ZARZĄDZANIA SYSTEMEM MONITORINGU WIZYJNEGO PŁYWALNI MIEJSKIEJ W KOLE

I. POSTANOWIENIA OGÓLNE

Polityka bezpieczeństwa przetwarzania danych osobowych zwana dalej „Polityką", została wydana w związku z § 3 ust. 1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

II. DOKUMENTY POWIĄZANE

1. Instrukcja bezpieczeństwa przetwarzania danych osobowych w systemie monitoringu wizyjnego Pływalni Miejskiej w Kole
2. Projekt systemu monitoringu wizyjnego Pływalni Miejskiej w Kole.

III. DEFINICJE

1. **Administrator danych** – Burmistrz Miasta Koła
2. **Administrator Bezpieczeństwa Informacji** – wyznaczona przez Administratora Danych Osobowych osoba, odpowiedzialna w szczególności za nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w systemie monitoringu wizyjnego oraz zbiorach nieinformatycznych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie ochrony danych osobowych.
3. **Administrator systemu monitoringu wizyjnego** – osoba, która otrzymuje zlecenie konserwacji czy naprawy sprzętu w przypadku takiej konieczności. Dostęp do systemu i infrastruktury monitoringu wizyjnego wymaga każdorazowej pisemnej zgody Kierownika Wydziału ds. obsługi krytej pływalni.

4. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołania się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.
5. **Osoba upoważniona** – osoba posiadająca formalne upoważnienie wydane przez Administratora danych lub przez osobę wyznaczoną (Administratora Bezpieczeństwa Informacji), uprawniona do przetwarzania danych osobowych.
6. **Przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.
7. **Rozporządzenie** – Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).
8. **Ustawa** – Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).
9. **Użytkownik systemu (operator/współpracownik)** – osoba upoważniona do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie monitoringu wizyjnego.
10. **Zbiór danych osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie.
11. **Monitoring wizyjny** – mamy na myśli ogół pomieszczeń Krytej Pływalni w Kole i pracowników zatrudnionych w Wydziale ds. obsługi krytej pływalni oraz zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
12. **Zbiór o nazwie „Monitoring wizyjny Pływalni Miejskiej w Kole"** - mamy na myśli zbiór danych osobowych zarejestrowany w GIODO, do którego dostęp mają pracownicy Wydziału ds. obsługi krytej pływalni w Kole, posiadający wydane przez Administratora Bezpieczeństwa Informacji upoważnienia do dostępu do danych zawartych w tym zbiorze.

13. **Operator systemu** – mamy na myśli pracownika Wydziału ds. obsługi krytej pływalni obsługującego w ramach swoich czynności służbowych system monitoringu wizyjnego.
14. **Kierownik** – mamy na myśli Kierownika Wydziału ds. obsługi krytej pływalni.
15. **Z–ca Kierownika** – mamy na myśli z–ce Kierownika Wydziału ds. obsługi krytej pływalni.
16. **Projekt systemu monitoringu wizyjnego** – dokument zawierający rozmieszczenie poszczególnych kamer oraz podstawowe informacje o ich parametrach, wykaz pomieszczeń lub ich części, w których przetwarzane są dane zarejestrowane przez kamery systemu, wykaz zbiorów zawierających dane zebrane w systemie, wykaz powiązań między nimi oraz wykaz programów i procedur służących do przetwarzania danych.

IV. ZAKRES ORAZ CEL POLITYKI

1. Celem polityki jest określenie podstawowych zasad właściwego zarządzania systemem monitoringu wizyjnego, służącym do przetwarzania danych osobowych oraz podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać wchodzące w jego skład, urządzenia, odpowiednio do zagrożeń i kategorii danych objętych ochroną.
2. Politykę stosuje się do danych osobowych przetwarzanych w systemach monitoringu wizyjnego, danych osobowych zapisanych w postaci elektronicznej na zewnętrznych nośnikach informacji oraz informacji o sposobach zabezpieczenia danych osobowych.
3. Przy przetwarzaniu danych osobowych w systemach monitoringu wizyjnego należy stosować wysoki poziom bezpieczeństwa w rozumieniu § 6 ust. 4 Rozporządzenia, ponieważ urządzenia systemu służącego do przetwarzania danych osobowych połączone są z siecią publiczną.
4. Polityka zawiera specyfikację podstawowych środków technicznych ochrony danych osobowych oraz elementów zarządzania systemem monitoringu wizyjnego. W przypadku, gdy z oceny funkcjonowania instrukcji wynika, że zachodzi potrzeba wprowadzenia nowych lub modyfikacji istniejących zasad właściwego zarządzania systemem monitoringu wizyjnego służącym do przetwarzania danych osobowych, wnioski w tej sprawie powinni składać użytkownicy systemu do Administratora Bezpieczeństwa Informacji za pośrednictwem Kierownika.

V. ZARZĄDZANIE OCHRONĄ DANYCH OSOBOWYCH

1. Administrator danych zabezpiecza dane osobowe przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Zasady określone w niniejszej Polityce oraz w dokumentach powiązanych powinny być znane i stosowane przez pracowników monitoringu miejskiego.
3. Pracownicy monitoringu miejskiego przed dopuszczeniem do przetwarzania danych osobowych, muszą zostać przeszkoleni w zakresie ochrony danych osobowych. Za opracowanie programu szkolenia i przeprowadzenie szkolenia odpowiada Administrator Bezpieczeństwa Informacji.
4. W imieniu Administratora danych nadzór nad przestrzeganiem zasad ochrony danych osobowych sprawuje Kierownik i jego zastępca.

VI. UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora Bezpieczeństwa Informacji wydawane indywidualnie przed rozpoczęciem przetwarzania danych osobowych i złożyły oświadczenie o zachowaniu w poufności danych i sposobów zabezpieczeń.
2. Upoważnienie wraz z oświadczeniem do przetwarzania danych osobowych obowiązuje do czasu ustania stosunku pracy lub obowiązków związanych z przetwarzaniem danych osobowych.
3. Upoważnienia wraz z oświadczeniem pracownika Wydziału ds. obsługi krytej pływalni, o których mowa powyżej przechowywane są w aktach osobowych pracownika oraz w dokumentacji Administratora Bezpieczeństwa Informacji.

VII. EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Ewidencja osób upoważnionych do przetwarzania danych osobowych jest prowadzona przez Administratora Bezpieczeństwa Informacji i zawiera:
   1) Imię i nazwisko osoby upoważnionej do przetwarzania danych osobowych.
   2) Zakres upoważnienia do przetwarzania danych osobowych.
   3) Datę nadania i odebrania uprawnień.

2. Przełożeni osób upoważnionych odpowiadają za natychmiastowe zgłoszenie do Administratora Bezpieczeństwa Informacji osób, które utraciły uprawnienia, które uzasadniały udzielenie im dostępu do danych osobowych.

VIII. OBSZARY PRZETWARZANIA DANYCH OSOBOWYCH

1. Dane osobowe mogą być przetwarzane wyłącznie w obszarach przetwarzania danych osobowych, na które składają się pomieszczenia monitoringu wizyjnego, zlokalizowane w budynku Pływalni Miejskiej w Kole. Do takich pomieszczeń, zalicza się:
   1) pomieszczenia, w których zlokalizowane są stacje robocze lub serwery służące do przetwarzania danych osobowych;
   2) pomieszczenia, w których przechowuje się zbiory nieinformatyczne, dokumenty źródłowe oraz wydruki z systemu monitoringu miejskiego zawierające dane osobowe;
   3) pomieszczenia, w których przechowywane są sprawne i uszkodzone urządzenia, elektroniczne nośniki informacji oraz kopie zapasowe zawierające dane osobowe.
2. Zbiory papierowe, wydruki i nośniki elektroniczne zawierające dane osobowe należy przechowywać w zamykanych szafach, które znajdują się w obszarach przetwarzania danych osobowych.
3. Niepotrzebne wydruki lub inne dokumenty należy niszczyć w niszczarkach.
4. Przebywanie wewnątrz obszarów przetwarzania danych osobowych osób nieuprawnionych jest dopuszczalne tylko w obecności i za zgodą Administratora danych, Sekretarza Miasta, Kierownika, z-cy Kierownika.

IX. WYKAZ ZBIORÓW DANYCH OSOBOWYCH

1. Zbiór danych osobowych „Monitoring wizyjny Pływalni Miejskiej w Kole" prowadzony jest w Wydziale ds. obsługi krytej pływalni.
2. Dane osobowe gromadzone we wskazanym zbiorze są przetwarzane w systemie monitoringu wizyjnego w pomieszczeniu należącym do obszaru przetwarzania danych osobowych.

X. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Powierzenie przetwarzania danych osobowych może mieć miejsce na podstawie pisemnej umowy określającej w szczególności zakres i cel przetwarzania danych. Umowa musi określać też zakres odpowiedzialności podmiotu, któremu powierzono przetwarzanie danych z tytułu niewykonania lub nienależytego wykonania umowy.
2. Powierzenie przetwarzania danych osobowych musi uwzględniać wymogi określone w art. 31 i nast. Ustawy. W szczególności podmiot zewnętrzny, któremu ma zostać powierzone przetwarzanie danych osobowych, jest obowiązany przed rozpoczęciem przetwarzania danych do podjęcia środków zabezpieczających zbiór danych, o których mowa w art. 36-39a Ustawy.
3. Powierzenie przetwarzania danych osobowych nie oznacza zwolnienia z odpowiedzialności Administratora danych i osób przez niego upoważnionych za zgodne z prawem przetwarzanie powierzonych danych, co wymaga w umowach stanowiących podstawę powierzenia przetwarzania danych umieszczenia prawa Administratora danych do kontroli wykonania przedmiotu umowy w siedzibie podmiotu zewnętrznego m. in. w zakresie przestrzegania Polityki, dokumentów powiązanych i właściwych przepisów prawa.

XI. UDOSTĘPNIANIE DANYCH OSOBOWYCH

1. Dane osobowe mogą być udostępniane zgodnie z przepisami prawa.
2. Udostępnianie danych osobowych może nastąpić wyłącznie za zgodą Kierownika. Zgoda, o ile nie zmieni się cel wykorzystania danych oraz podmiot, któremu dane są udostępniane, może obejmować także przypadki udostępnienia danych w przyszłości.
3. Udostępniając dane osobowe innym podmiotom należy odnotowywać informacje o ich udostępnieniu.
4. W przypadku przekazywania urządzeń lub nośników zawierających dane osobowe w tym dane wrażliwe, poza obszar przetwarzania danych osobowych, zabezpiecza się je w sposób zapewniający poufność, integralność i rozliczalność tych danych.
5. Umożliwia się przekazywanie i wgląd do danych ze zbioru danych upoważnionym do tego służbom (Policja, Straż Miejska, Prokuratura, Sąd) na podstawie pisemnego wniosku kierownika danej jednostki.
6. Dane osobowe ze zbioru „Monitoring wizyjny Pływalni Miejskiej w Kole" przekazywane są na nośnikach zewnętrznych w postaci płyty CD lub DVD wyłącznie upoważnionym do tego służbom (Policja, Straż Miejska, Prokuratura, Sąd) .

7. Przekazanie danych osobowych odbywa się tylko i wyłącznie poprzez osoby do tego uprawnione tj.: Kierownika oraz jego Z-cy.
8. Przekazanie nośników odbywa się na podstawie protokołu przekazania, który ewidencjonowany jest w aktach sprawy.
9. Przekazane dane są dodatkowo kopiowane i zabezpieczane w stacji monitoringu w postaci takiej samej płyty CD lub DVD w celu zabezpieczenia przed jego ewentualnym zniszczeniem, skasowaniem itp.
10. Archiwizowany w pomieszczeniach monitoringu skopiowany nośnik jest odpowiednio zabezpieczony przed dostępem nieuprawnionych osób. Nośnik zostaje odpowiednio opisany (charakter, miejsce i czas zdarzenia), ponumerowany oraz zabezpieczony w szafie zamykanej na klucz. Dostęp do szafy mają: Kierownik oraz jego z-ca.

XII. ŚRODKI ORGANIZACYJNE I TECHNICZNE

Dane osobowe są chronione przy zastosowaniu następujących zabezpieczeń niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych dany osobowych:

1. Ochrona pomieszczeń wykorzystanych do przetwarzania danych osobowych:
   1) budynek i wszystkie pomieszczenia, w których zlokalizowano przetwarzanie danych osobowych zabezpieczone są przed dostępem osób nieuprawnionych poprzez ograniczony dostęp do pomieszczeń przetwarzania danych osobowych oraz innych środków opisanych w Instrukcji bezpieczeństwa przetwarzania danych osobowych w systemie monitoringu miejskiego
   2) dokumentacja papierowa po godzinach pracy osób upoważnionych do jej przetwarzania jest przechowywana w zamykanych biurkach i szafach;
   3) przebywanie osób nieuprawnionych w obszarze przetwarzania danych osobowych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych lub za zgodą wyznaczonej osoby.
2. Przedsięwzięcia w zakresie zabezpieczenia sprzętu komputerowego:
   1) dla zapewnienia ciągłości działania systemu monitoringu wizyjnego służącego do przetwarzania danych osobowych stosuje się sprzęt i oprogramowanie wyprodukowane przez renomowanych producentów
   2) programy służące do przetwarzania danych osobowych są zabezpieczane przed przypadkową utratą albo celowym zniszczeniem.

3. Przedsięwzięcia w zakresie ochrony teletransmisji danych:
   1) w celu ochrony systemu monitoringu wizyjnego służącego do przetwarzania danych osobowych przed zagrożeniami pochodzącymi z Internetu stosuje się zabezpieczenia chroniące przed nieuprawnionym dostępem;
   2) transmisja danych osobowych przez publiczną sieć telekomunikacyjną jest zabezpieczona środkami kryptograficznej ochrony danych;
4. Przedsięwzięcia w zakresie środków ochrony w ramach oprogramowania systemów w celu zapewnienia rozliczalności operacji dokonywanych przez użytkowników systemu monitoringu miejskiego prowadzona jest książka służby, w której odnotowywane są data i godziny pracy, imiona i nazwiska operatorów;
5. Przedsięwzięcia w zakresie środków ochrony w ramach systemu użytkowego:
   1) w celu ochrony danych osobowych przetwarzanych na stacjach roboczych na czas krótkotrwałego opuszczenia stanowiska pracy przez operatora, pomieszczenie obserwacyjne zamykane jest na klucz;
   2) na stacji roboczej użytkownik nie posiadają uprawnień do instalowania nieautoryzowanego oprogramowania;
   3) stosuje się oprogramowanie antywirusowe z automatyczną aktualizacją w celu ochrony systemu przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu monitoringu miejskiego;
   4) kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie jak i do celów instalacyjnych.
6. Przedsięwzięcia w zakresie środków organizacyjnych.
   1) wyznaczono Administratora Bezpieczeństwa Informacji;
   2) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych;
   3) dostęp do danych osobowych możliwy jest po uzyskaniu zgody do dostępu do danych osobowych wydanego przez upoważnione osoby i w ich obecności;
   4) wprowadzono Instrukcję zarządzania systemem monitoringu wizyjnego służącym do przetwarzania danych osobowych;
   5) monitoruje się wdrożone zabezpieczenia systemu monitoringu wizyjnego.

XIII. ZGONOŚĆ

1. Niniejsza Polityka oraz dokumenty powiązane powinny być aktualizowane wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w ramach Administratora danych, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.
2. Okresowy przegląd Polityki powinien mieć na celu stwierdzenie, czy postanowienia Polityki odpowiadają aktualnej i planowanej działalności Administratora danych oraz są prawnie aktualne w momencie dokonywania przeglądu.
3. Zmiany niniejszej Polityki wymagają przeglądu innych dokumentów dotyczących ochrony danych osobowych obowiązujących u Administratora danych.
4. Politykę bezpieczeństwa oraz zmiany Polityki bezpieczeństwa wprowadza się w życie w formie zarządzenia Burmistrza Miasta Koła.

XIV. POSTANOWIENIA KOŃCOWE

1. Naruszenie zasad określonych w niniejszej Polityce może być podstawą rozwiązania stosunku pracy, zgodnie z Kodeksem Pracy
2. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.) oraz przepisy wykonawcze do tej Ustawy.
3. Pracownicy Administratora danych zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce. W wypadku uregulowań występujących w innych niż niniejsza Polityka procedurach obowiązujących u Administratora danych, użytkownicy mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.

BURMISTRZ
Mieczysław Drożdżewski

ADMINISTRATOR
Bezpieczeństwa Informacji
Andrzej Bednarkiewicz