

ZARZĄDZENIE NR 23/2016
BURMISTRZA DOBREJ

z dnia 1 września 2016 r.

**w sprawie wdrożenia do stosowania dokumentacji przetwarzania i ochrony danych osobowych
z systemu monitoringu wizyjnego w Dobrej**

Na podstawie art. 31 oraz art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (j.t. Dz.U. z 2016 r., poz. 446), w związku z art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (j.t. Dz. U. z 2016 r., poz. 922) oraz § 3 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 informacyjne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024), Burmistrz Dobrej zarządza, co następuje:

§ 1.

1. Wprowadzam do stosowania „Politykę bezpieczeństwa przetwarzania danych osobowych z systemu monitoringu wizyjnego w Dobrej”, w brzmieniu stanowiącym załącznik nr 1 do Zarządzenia.

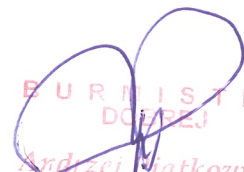
2. Wprowadzam do stosowania „Plan systemu monitoringu wizyjnego w Dobrej”, w brzmieniu stanowiącym załącznik nr 2 do Zarządzenia.

§ 2.

Wykonanie zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji.

§ 3.

Zarządzenie wchodzi w życie z dniem podpisania.


BURMISTRZ
DOBREJ
Andrzej Łątkowski

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH

Z SYSTEMU MONITORINGU W DOBREJ

I. Postanowienie ogólne.

1. 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 system monitoringu służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024).

II. Dokumenty powiązane.

1. Zarządzenie nr 15/2011 Burmistrza Dobrej z dnia 01 czerwca 2011 r. w sprawie wprowadzenia i wdrożenia do stosowania Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz Polityki bezpieczeństwa danych osobowych .

2. Plan systemu monitoringu w Dobrej.

III. Definicje.

1. Urząd - należy przez to rozumieć Urząd Miejski w Dobrej.
2. Administrator danych - należy przez to rozumieć Burmistrza Dobrej.
3. Administrator Bezpieczeństwa Informacji - należy przez to rozumieć pracownika urzędu lub inną osobę wyznaczoną do nadzorowania przestrzegania zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych.
4. Administrator systemu monitoringu wizyjnego - wyznaczona osoba odpowiedzialna za funkcjonowanie infrastruktury systemu monitoringu, za ich przeglądy, konserwację oraz za stosowanie technicznych i organizacyjnych środków bezpieczeństwa w systemie monitoringu.
5. 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 identyfikujący, 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.
6. Osoba upoważniona - osoba posiadająca formalne upoważnienie wydane przez Administratora danych lub przez osobę wyznaczoną, uprawniona do przetwarzania danych osobowych.
7. Przetwarzanie danych osobowych - jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.
8. 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 system monitoringu miejskiego służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).

9. Ustawa - Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (j.t. Dz.U. z 2016 r., poz. 922).
10. Użytkownik systemu (operator/współpracownik) - osoba upoważniona do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie monitoringu.
11. 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.
12. Pomieszczenie monitoringu w Dobrej -
 - 1) pokój nr 7 w budynku Komisariatu Policji w Dobrej przy ul. Dekerta 29
 - 2) pokój nr w budynku Zespołu Szkolno – Przedszkolnego w Dobrej, Długa Wieś 28
gdzie znajdują się rejestratory i monitory, na którym odtwarzany jest obraz kamer.
13. Monitoring miejski - pomieszczenia i osoby upoważnione do przetwarzania danych osobowych pozyskiwanych z obrazów przesyłanych przez kamery oraz zespół współpracujących urzędów, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
14. Plan systemu monitoringu wizyjnego w Dobrej- 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.
15. Zdarzenie - każda sytuacja zdefiniowana przez użytkownika systemu CCTV, którą system powinien wykryć i/lub na nią zareagować, np. przestępstwo, awaria instalacji, naruszenie przestrzeni prywatnej, działanie pracownika niezgodne z procedurą, itd.
16. Przestrzeń publiczna - przestrzeń, do której użytkownicy mają nieograniczony dostęp, np. przestrzeń na terenie miasta Dobra lub droga publiczna.
17. Przestrzeń pół-publiczna - przestrzeń prywatna, udostępniona innym osobom na warunkach określonych przez właściciela.
18. Konstytucyjna zasada proporcjonalności - w odniesieniu do systemów monitoringu wizyjnego, jest to taki zakres prowadzonej obserwacji, rejestracji obrazu, przechowywania nagrań i przetwarzania danych z systemu CCTV, który umożliwia realizację celów przez właściciela lub zarządzającego obszarem objętym nadzorem i w jak najmniejszy sposób narusza prawa i wolność osób, które znajdują się na tym obszarze.

IV. Zakres oraz cel polityki.

1. Celem polityki jest określenie podstawowych zasad właściwego zarządzania systemem monitoringu, 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 systemie monitoringu, danych osobowych zapisanych w postaci elektronicznej na zewnętrznych nośnikach informacji oraz informacji o sposobach zabezpieczenia danych osobowych, o których mowa w art. 39 ust. 3 ustawy.

3. Polityka zawiera specyfikację podstawowych środków technicznych ochrony danych osobowych oraz elementów zarządzania systemem monitoringu. W przypadku, gdy z oceny funkcjonowania instrukcji wynika, że zachodzi potrzeba wprowadzenia nowych lub modyfikacji istniejących zasad właściwego zarządzania systemem monitoringu, służącym do przetwarzania danych osobowych, wnioski w tej sprawie powinni składać użytkownicy systemu do Administratora Systemu Monitoringu.

V. Zarządzanie ochroną danych osobowych.

1. Obserwacja i zapis obrazu na elektronicznych nośnikach informacji - oprócz doraźnego celu, jakim jest obserwacja, istnieją inne cele np. zapamiętanie obrazu dla celów dowodowych, lub zapewnienie możliwości ponownej jego obserwacji w celu przyjrzenia się jego szczegółom.

2. Zapisywanie obrazu odbywa się w celu zapewnienia możliwości jego odtworzenia w przyszłości - rejestracja obrazu służy głównie celom dowodowym i prewencyjnym tj. zniechęcającym do popełnienia zabronionych czynów na skutek łatwych możliwości ich wykrycia.

3. Dane zapisywane w systemie przechowywane są nie dłużej niż 14 dni.

4. Administrator danych zabezpiecza dane osobowe przed ich udostępnianiem osobom nieupoważnionym, zabraniam przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

5. Zasady określone w niniejszej Polityce oraz w dokumentach powiązanych powinny być znane i stosowane przez pracowników monitoringu.

6. Pracownicy monitoringu przed dopuszczeniem do przetwarzania danych osobowych, zostają zapoznani z przepisami z zakresu ochrony danych osobowych.

7. W imieniu Administratora danych nadzór nad przestrzeganiem zasad ochrony danych osobowych sprawuje Administrator Systemu Monitoringu.

VI. Upoważnienie do przetwarzania danych osobowych.

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora danych wydawane indywidualnie przed rozpoczęciem przetwarzania danych osobowych.

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, o których mowa powyżej przechowywane są w aktach osobowych pracownika.

VII. Ewidencja osób upoważnionych do przetwarzania danych osobowych.

1. Ewidencja osób upoważnionych do przetwarzania danych osobowych jest prowadzona przez Administratora Bezpieczeństwa Informacji lub osobę przez niego wyznaczoną 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 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. Do takich pomieszczeń zalicza się:

- 1) pomieszczenia, w których zlokalizowane są rejestratory,
- 2) gabinet Burmistrza,
- 3) pomieszczenia, w których przechowywane są sprawne i uszkodzone urządzenia, elektroniczne nośniki informacji oraz kopie zapasowe zawierające dane osobowe.

2. Nośniki elektroniczne zawierające dane osobowe należy przechowywać w zamkniętych szafach, które znajdują się w obszarach przetwarzania danych osobowych.

IX. Wykaz zbiorów danych osobowych.

Dane osobowe z monitoringu wizyjnego gromadzone są w zbiorze pn „Monitoring wizyjny w Dobrej” zarejestrowanym przez Administratora Bezpieczeństwa Informacji w prowadzonym przez niego rejestrze. Dane osobowe gromadzone we wskazanym zbiorze są przetwarzane w systemie monitoringu, które są zlokalizowane w pomieszczeniach należących 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 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 przetwarzanych 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 art. 27 ust. 2 pkt 1-5 Ustawy.
2. Udostępnianie danych osobowych może nastąpić wyłącznie za zgodą Administratora danych. Zgoda, o ile nie zmieni się cel wykorzystania danych oraz podmiot, któremu dane są udostępniane, może obejmować także przypadki udostępniania danych w przyszłości.
3. Udostępniając dane osobowe innym podmiotom należy odnotować 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 rozłączalność tych danych.
5. Umożliwia się przekazywanie i wgląd do danych ze zbioru danych upoważnionym do tego służbom (Policja, Prokuratura, Sąd) na podstawie pisemnego wniosku kierownika danej jednostki.
6. Dane osobowe ze zbioru „Monitoring wizyjny” przekazywane są na nośnikach zewnętrznych w postaci płyty CD lub DVD wyłącznie upoważnionym do tego służbom (Policja, Prokuratura, Sąd).
7. Przekazywanie danych osobowych odbywa się tylko i wyłącznie przez osoby do tego upoważnione.
8. Prowadzony jest odpowiedni rejestr wydawanych nośników.
9. 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 zamkniętej na klucz. Dostęp do szafy ma Administrator Systemu Monitoringu.

XII. Środki techniczne i organizacyjne.

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

1. Ochrona pomieszczeń wykorzystanych do przetwarzania danych osobowych:
 - 1) budynek i wszelkie pomieszczenia, w których zlokalizowano przetwarzanie danych osobowych zabezpieczone są przed dostępem osób nieuprawnionych,
 - 2) przebywanie osób nieuprawnionych w obszarze przetwarzania danych osobowych jest dopuszczalne za zgodą wyznaczonej osoby Administratora Monitoringu.
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 oraz zabezpiecza się sprzęt przed awarią zasilania lub zakłóceniami w sieci zasilającej; Jedynie urządzenia firmy Mikrotik wykrywają protokół nv2,
3. Przedsięwzięcia w zakresie środków ochrony w ramach systemu użytkowego:
 - 2) Przesył danych osobowych odbywa się wydzieloną siecią bez dostępu do Internetu .
 - 3) Zarządzanie siecią odbywa się z Centrum Monitoringu,
 - 4) W ramach zabezpieczeń programowych użyto protokołu szyfrowania transmisji,
4. 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 wydanej przez upoważnione osoby i w ich obecności,
 - 4) wprowadzono Instrukcję zarządzania systemem monitoringu służącym do przetwarzania danych osobowych,
 - 5) monitoruje się wdrożone zabezpieczenia systemu monitoringu.

XIII. Zgodność.

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 Dobrej.

XIV. Postanowienia końcowe.

1. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (j.t. Dz.U. z 2016 r., poz. 922) oraz przepisy wykonawcze do tej Ustawy.

2. Pracownicy 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.

B U R M I S T R Z
DOBREJ

Andrzej Piątkowski

PLAN SYSTEMU MONITORINGU WIZYJNEGO W DOBREJ

I. Ogólna charakterystyka systemu .

Łącznie w systemie monitoringu wizyjnego w Dobrej pracuje 6 kamer (od PK1 do PK 6) w 3 punktach kamerowych. System monitoringu funkcjonuje w oparciu o dwa systemy – przewodowy i bezprzewodowy. W/w system monitoringu obsługiwany jest przez przeszkolonych operatorów.

II. Stanowiska operatorskie.

Pomieszczenie systemu monitoringu dla punktów kamerowych PK 1 i PK 2 znajdują się w budynku Komisariatu Policji w Dobrej – pok. nr 7. Dla PK 3 pomieszczenie systemu monitoringu znajduje się w budynku Zespołu Szkolno – Przedszkolnego w Dobrej : gabinet Dyrektora Zespołu.

Pomieszczenia systemu monitoringu zabezpieczone są przed dostępem osób postronnych. Wideorejestratory znajdują się w zamykanych szafach.

III. Charakterystyka techniczna systemu monitoringu.

1. Kamery monitoringu wizyjnego posiadają następujące parametry:

- 1) kamery tubowe - 3 szt (2 szt – PK 1, PK 3; 1 szt- PK 5) : BCS-P-462RWSA , dzień/noc, obiektyw 2.8-12 mm F1.6 MOTOZOOM, przetwornik 1/3” 2 Megapixel CMOS, kodowanie H.264&MJPEG, obsługa trzech strumieni kodowania, mechaniczny filtr podczerwieni (specyfikacja urządzenia stanowi załącznik nr 1),
- 2) kamery tubowe – 2 szt. (PK 2, PK 6) . : BCS-TIP7130AIR 1, 3 Megapixels ze zmiennym ogniskowym obiektywem, obiekty 7-22 mm F1.4. auto DC, przetwornik 1/3” 2 Megapixel CMOS, kodowanie H.264&MJPEG, obsługa dwóch strumieni kodowania , mechaniczny filtr podczerwieni (specyfikacja urządzenia stanowi załącznik nr 2),
- 3) kamera tubowa - 1 szt (PK 4), BSC-TIP7200AIR , obiektyw 7-22 mm F1.4 auto DC, przetwornik 1/2,8” 2 Megapixel CMOS, kodowanie H.264&MJPEG, obsługa dwóch strumieni kodowania, mechaniczny filtr podczerwieni (specyfikacja urządzenia stanowi załącznik nr 3),

2. Rejestrator cyfrowy BCS-P-NVR1602 - 16 kanałowy sterowany przy pomocy myszy i klawiatury (specyfikacja urządzenia stanowi załącznik nr 4)

3. Kamery systemu monitoringu nie posiadają wbudowanych mechanizmów przetwarzania danych, wykrywania obiektów, identyfikacji, kierunku przemieszczania itp.

4. Kamery systemu monitoringu (6 szt.) są kamerami stałymi, bez możliwości obrotu, mającymi możliwość zbliżania i oddalania, przez co szczegółowej obserwacji wybranego obiektu, będącego w rejonie zasięgu danej kamery.

IV. Rozmieszczenie kamer monitoringu.

Kamery monitoringu zlokalizowane są przy skrzyżowaniu głównych ciągów komunikacyjnych oraz w sąsiedztwie dwóch parków miejskich . System monitoringu stworzony został w oparciu o analizę miejsc najbardziej zagrożonych. Zlokalizowanie kamer zostało przedstawione na załączniku nr 5 do niniejszego planu.

Rozmieszczenie kamer na terenie Dobrej jest następujące:

1. Skrzyżowanie Placu Wojska Polskiego i ul. Kilińskiego oraz ul. Dekerta ;
2. Wschodnia ściana budynku Centrum Kultury w Dobrej z obszarem kaperowanym parku miejskiego w Dobrej
3. Zachodnia ściana budynku Hali Sportowej w Długiej Wsi z obszarem kaperowanym parku miejskiego w Długiej Wsi ;

V. Sposoby przesyłu wizji.

1. Przesył wizji z poszczególnych kamer odbywa się drogą radiową oraz za pomocą światłowodów.

VI. Informacje końcowe.

1. Polityka bezpieczeństwa przetwarzania danych osobowych monitoringu wizyjnego w Dobrej stanowi integralną część planu. Plan będzie podlegał bieżącej modyfikacji w chwili instalacji nowych kamer, stanowisk, stacji bazowych, zmianę oprogramowania, sposobu przesyłu danych itp.

BURMISTRZ
DOBREJ
Andrzej Piątkowski