ZARZĄDZENIE NR 10/14
BURMISTRZA STRONIA ŚLĄSKIEGO

z dnia 10 grudnia 2014 r.

w sprawie wdrożenia dokumentacji przetwarzania i ochrony danych osobowych z systemu monitoringu wizyjnego w Stroniu Śląskim.

Na podstawie art. 31 oraz art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (j.t. Dz.U. z 2013 r., poz. 594 ze zm.), w związku z art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (j.t. Dz. U. z 2014 r., poz. 1182) 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 Stronia Śląskiego zarządza, co następuje:

§ 1. 1. Wprowadzam do stosowania „**Politykę bezpieczeństwa przetwarzania danych osobowych z systemu monitoringu wizyjnego w Stroniu Śląskim",** w brzmieniu stanowiącym załącznik nr 1 do Zarządzenia.

2. Wprowadzam do stosowania **„Plan systemu monitoringu wizyjnego w Stroniu Śląskim",** w brzmieniu stanowiącym załącznik nr 2 do Zarządzenia.

§ 2. Wykonanie zarządzenia powierzam Sekretarzowi Gminy.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik Nr 1 do Zarządzenia Nr 10/14

Burmistrza Stronia Śląskiego

z dnia 10 grudnia 2014 r.

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH Z SYSTEMU MONITORINGU W STRONIU ŚLĄSKIM

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

II. Dokumenty powiązane.

1. Zarządzenie nr 115/11 Burmistrza Stronia Śląskiego z dnia 21 czerwca 2011 r. (ze zmianami) w sprawie wprowadzenia do użytku służbowego „Polityki bezpieczeństwa informacji" oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" w Urzędzie Miejskim w Stroniu Śląskim.

2. Plan systemu monitoringu w Stroniu Śląskim.

III. Definicje.

1. **Urząd -** należy przez to rozumieć Urząd Miejski w Stroniu Śląskim.

2. **Administrator danych –** należy przez to rozumieć Burmistrza Stronia Śląskiego.

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** - jakiekolwiek 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 2014 r., poz. 1182).

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 Stroniu Śląskim -** pokój nr 1 w budynku w Stroniu Śląskim przy ul. Mickiewicza 2, gdzie znajduje się rejestrator i monitory, na którym odtwarzany jest obraz kamer.

13. **Monitoring miejski -** pomieszczenia i pracownicy zatrudnieni w Straży Miejskiej w Stroniu Śląskim oraz zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

14. **Projekt systemu monitoringu w Stroniu Śląskim –** 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 Stronia Śląskiego 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 24 dni.

4. 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.

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, muszą zostać przeszkoleni w zakresie ochrony danych osobowych. Za opracowanie programu szkolenia i przeprowadzenie szkolenia odpowiada Administrator Bezpieczeństwa Informacji.

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

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) pomieszczenie, w którym zlokalizowany jest rejestrator,

2) gabinet Burmistrza,

3) pomieszczenia, w których przechowuje się zbiory nieinformatyczne, dokumenty źródłowe oraz wydruki z systemu monitoringu zawierające dane osobowe,

4) 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.

IX. Wykaz zbiorów danych osobowych.

Dane osobowe gromadzone we wskazanym zbiorze są przetwarzane w systemie monitoringu oraz w rejestrach nieinformatycznych, które są zlokalizowane w pomieszczeniach należących do obszaru przetwarzania danych osobowych.

X. Powierzanie 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, Straż Miejska, 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, Straż Miejska, Prokuratura, Sąd).

7. Przekazywanie danych osobowych odbywa się tylko i wyłącznie przez osoby do tego upoważnione.

8. Prowadzony jest odpowiedni rejestr wydawanych nośników.

9. Przekazane dane mogą być kopiowane i zabezpieczane w stacji monitoringu w postaci takiej samej płyty CD lub DVD w celu zabezpieczenia przed jego ewentualnym zniszczeniem, skasowaniem itp. Fakt wykonania kopii odnotowany jest w dokumentach dotyczących przekazania danych innym organom.

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 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) 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 za zgodą wyznaczonej osoby Administratora danych.

2. Przedsięwzięcia w zakresie zabezpieczenia sprzętu komputerowego:

1) dla zapewnienia ciągłości działania systemu CCTV 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;

3. Przedsięwzięcia w zakresie środków ochrony w ramach systemu użytkowego:

1) na stacjach roboczych użytkownicy nie posiadają uprawnień do instalowania nieautoryzowanego oprogramowania,

2) stosuje się oprogramowanie antywirusowe z automatyczną aktualizacją w celu ochrony systemu przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu monitoringu;

3) kontrola antywirusowa jest przeprowadzona na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie jak i do celów instalacyjnych.

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 wydanego przez upoważnione osoby i w ich obecności,

4) wprowadzono Instrukcję zarządzania systemem monitoringu służącym do przetwarzania danych osobowych,

5) monitoruje się wdrożone zabezpieczenia systemu CCTV.

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 Stronia Śląskiego.

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 2014 r., poz. 1182) 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.

Załącznik Nr 2 do Zarządzenia Nr 10/14

Burmistrza Stronia Śląskiego

z dnia 10 grudnia 2014 r.

PLAN SYSTEMU MONITORINGU WIZYJNEGO W STRONIU ŚLĄSKIM

I. Ogólna charakterystyka systemu CCTV.

Łącznie w systemie monitoringu wizyjnego w Stroniu Śląskim pracuje 9 kamer. System monitoringu funkcjonuje w oparciu o jeden system – przewodowy. W/w system monitoringu obsługiwany jest przez przeszkolonych pracowników.

II. Stanowiska operatorskie.

Pomieszczenia systemu monitoringu zabezpieczone są przed dostępem osób postronnych. Wideorejestrator znajduje się w zamykanej szafie.

III. Charakterystyka techniczna systemu monitoringu.

1. Kamery monitoringu wizyjnego posiadają następujące parametry: kamery obrotowe 9 szt VG 4-300 BOSCH, dzień/noc, 470 linii, zoom optyczny 18 x 200 cm optyczny, tryb kolorowy dzień/monochromatyczny noc, 15 tras programowalnych.

2. Rejestrator cyfrowy 16 kanałowy, zaawansowana wideo detekcja, rozdzielczość P60 H, kompresja H.264;G711, sterowanie przy pomocy myszy i klawiatury BOSCH IntuiKey KBD-DIGITAL.

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

4. Kamery systemu CCTV- 9 szt. są kamerami obrotowymi, mającymi możliwość zbliżania i oddalania, przez co szczegółowej obserwacji wybranego obiektu, będącego w rejonie zasięgu danej kamery. Poruszają się automatycznie lub przez operatora.

IV. Rozmieszczenie kamer monitoringu.

Kamery monitoringu zlokalizowane są na skrzyżowaniach głównych ciągów komunikacyjnych. System monitoringu rozwijany jest w oparciu o analizę miejsc najbardziej zagrożonych.

Rozmieszczenie kamer na terenie Stronia Śląskiego jest następując:

1. ul. Kościuszki, budynek nr 20 (skrzyżowanie ulic: Dolna, Hutnicza, Kościuszki);
2. ul. Zielona, budynek nr 3 (skrzyżowanie ulic: Zielona, Nadbrzeżna);
3. ul. Mickiewicza, budynek nr 2 (skrzyżowanie ulic: Nadbrzeżna, Mickiewicza, Kościuszki);
4. ul. Kościuszki, budynek nr 33b (skrzyżowanie ulic: Górna, Kościuszki);
5. rondo (skrzyżowanie ulic: Sudecka, Nadbrzeżna, Kościuszki);
6. ul. Kościuszki przy budynku nr 57 (ul.: Kościuszki, Szkoła Podstawowa, Park Morawka);
7. ul. Morawka budynek nr 30 (skrzyżowanie ulic: Morawka, Nowotki);
8. ul. Kościuszki budynek nr 70 (zapora, skrzyżowanie ulic: Kościuszki, Świerczewskiego);
9. Park Miejski przy Urzędzie Miejskim w Stroniu Śląskim.

VI. Sposoby przesyłu wizji.

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

VII. Informacje końcowe.

1. Polityka bezpieczeństwa przetwarzania danych osobowych monitoringu wizyjnego w Stroniu Śląskim stanowi integralną część planu.

Plan będzie podlegał bieżącej modyfikacji w chwili instalacji nowych kamer, stanowisk, stacji bazowych, zmiany oprogramowania, sposobu przesyłu danych itp.