ZARZĄDZENIE NR 21.2018.K
PREZYDENTA MIASTA ZIELONA GÓRA
- KIEROWNIKA URZĘDU

z dnia 3 października 2018 r.

w sprawie polityki zarządzania systemem ochrony wizyjnej w Urzędzie Miasta Zielona Góra.

Na podstawie art. 9a, 33 ust. 3 i 5 ustawy z dnia 8 marca 1990 r. *o samorządzie gminnym* (Dz. U. z 2018 r. poz. 994 z późn. zm.[1)]) i art. 4b, art. 92 ust. 1 pkt 2 i ust. 2 ustawy z dnia 5 czerwca 1998 r. *o samorządzie powiatowym* (Dz. U. z 2018 r. poz. 995 z późn. zm.[2)]), art.6. ust. 1 lit. e oraz art. 24 ust. 1 i 2 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* (Dz. U. UE L119 z 04.05.2016) **zarządza się, co następuje:**

Rozdział 1
Przepisy ogólne

§ 1. Zarządzenie określa zasady funkcjonowania systemu ochrony wizyjnej miasta Zielona Góra zarządzanej przez Urząd Miasta Zielona Góra, reguły rejestracji i zapisu informacji oraz sposób ich zabezpieczenia, a także możliwości udostępniania zgromadzonych danych o zdarzeniach – zwane dalej „polityką".

§ 2. Polityka ma zastosowanie tylko do realizacji zadań z zakresu ochrony wizyjnej oraz do czynności stanowiących przetwarzanie danych osobowych za pomocą systemu ochrony wizyjnej.

§ 3. Polityka nie wyłącza zastosowania odrębnych przepisów w zakresie zasad postępowania wynikających aktów prawnych, ze świadczenia pracy, w tym przepisów przeciwpożarowych, bezpieczeństwa i higieny pracy lub regulaminów.

§ 4. 1. Zarządzenie używa sformułowań:

1) „*administrator danych osobowych, inspektor ochrony danych (IOD)*, *odbiorca danych, usuwanie danych, system ochrony wizyjnej (informatyczny), zabezpieczenie systemu ochrony wizyjnej (informatycznego)"* w rozumieniu 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*;

2) *„sieć publiczna, sieć telekomunikacyjna"* w rozumieniu przepisów o telekomunikacji.

2. Ilekroć w zarządzeniu jest mowa o:

1) *ustawie* – należy przez to rozumieć ustawę *o ochronie danych osobowych;*

2) *RODO* - należy przez to rozumieć *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);*

3) *administratorze OW* - należy przez to rozumieć pracownika zarządzającego systemem ochrony wizyjnej, odpowiedzialnego za techniczną i merytoryczną eksploatację systemu;

4) *centrum monitoringu* - należy przez to rozumieć pomieszczenia urzędu zlokalizowane przy ul. Jana Kasprowicza 3/5 w Zielonej Górze;

5) *użytkowników* OW – należy przez to rozumieć: pracowników Urzędu Miasta Zielona Góra - stanowisk obsługi i systemów pomocniczych lub pracowników innych podmiotów zewnętrznych - uprawnionych do korzystania z systemu ochrony wizyjnej podczas wykonywania obowiązków służbowych;

[1)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 1000,1349 i 1432.
[2)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 1000,1349 i 1432.

6) *osobie upoważnionej* OW – należy przez to rozumieć osobę zatrudnioną na podstawie umowy o pracę, umowy zlecenia lub innej umowy w zakresie ochrony wizyjnej, której nadane zostało przez administratora danych upoważnienie do przetwarzania danych osobowych dotyczące systemu ochrony wizyjnej w zakresie wskazanym w upoważnieniu;
7) *integralności danych* OW– należy przez to rozumieć właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
8) *poufności danych* OW– należy przez to rozumieć właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
9) *uwierzytelnianiu* OW – należy przez to rozumieć działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
10) *urządzeniu komputerowym* OW – należy przez to rozumieć urządzenie techniczne, będące częścią systemu ochrony wizyjnej, mogące służyć do wprowadzania, wyprowadzania, przekazywania, przetwarzania danych osobowych;
11) *teletransmisji* OW– należy przez to rozumieć przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
12) *komórce IT* – należy przez to rozumieć komórkę organizacyjną urzędu właściwą ds. obsługi informatycznej Urzędu Miasta Zielona Góra;
13) *CCTV*- (Closed-Circuit TeleVision) należy przez to rozumieć systemy ochrony wizyjnej;

§ 5. 1. Na terenie Miasta Zielona Góra funkcjonują całodobowo techniczne urządzenia monitorujące obszar ograniczony granicami terytorialnymi miasta i zarządzane przez Urząd Miasta Zielona Góra.
2. Lokalizacja kamer ochrony wizyjnej jest wizualizowana w postaci mapy przez kierownika kom. org. urz. właściwej ds. monitoringu.

§ 6. System ochrony wizyjnej miasta Zielona Góra składa się z:
1) kamer rejestrujących zdarzenia w kolorze i rozdzielczości umożliwiających identyfikację osób;
2) urządzeń rejestrującego i zapisującego obraz na nośniku fizycznym (dysk twardy);
3) stanowisk oglądu bieżącego i pozwalającego na przeglądanie rejestrowanych zdarzeń.

§ 7. Rejestracji i zapisaniu na nośniku fizycznym podlega tylko obraz (wizja) z kamer systemu monitoringu. Nie rejestruje się dźwięku (fonii).

§ 8. Do rejestracji obrazu służą urządzenia wchodzące w skład systemu rejestracji spełniającego wymogi określone Polską Normą PN-EN 50132-7 dla systemów dozorowanych CCTV.

§ 9. Uwzględniając kategorie danych osobowych, skalę przetwarzania danych osobowych oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie ochrony wizyjnej połączonym z siecią publiczną, stosuje się środki techniczne i organizacyjne zapewniające możliwy do osiągnięcia poziom zabezpieczeń systemu OW.

Rozdział 2
Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie ochrony wizyjnej

§ 10. Zadania w zakresie koordynacji zakupu, technicznego wdrożenia, utrzymania zdolności, zarządzania użytkownikami i zapewnienia bezpieczeństwa systemu ochrony wizyjnej realizuje kierownik komórki organizacyjnej właściwej ds. monitoringu będący jednocześnie administratorem OW.

§ 11. Zadania określone w § 10 realizuje administrator systemu OW zgodnie z regulaminem wewnętrznym kom. org. urz. właściwej ds. bezpieczeństwa i zarządzania kryzysowego.

§ 12. 1. Dostęp do przetwarzania danych osobowych w systemie ochrony wizyjnej mogą mieć wyłącznie osoby, którzy posiadają upoważnienie administratora danych osobowych do przetwarzania danych osobowych i odpowiednie uprawnienia.
2. Zakres dostępu do danych osobowych przetwarzanych w systemie ochrony wizyjnej nie może być szerszy niż w wydanym upoważnieniu.

§ 13. 1. Rejestracja użytkownika OW w systemie ochrony wizyjnej oraz nadanie uprawnień następuje przez administratora OW po uzyskaniu upoważnienia do przetwarzania danych osobowych przez osobę zgodnie z odrębnymi przepisami;

2. Zakres uprawnień dla użytkownika OW systemu ochrony wizyjnej określa kierownik kom. org. urz. właściwej ds. monitoringu.

§ 14. 1. Wyrejestrowania użytkownika OW z systemu ochrony wizyjnej dokonuje administrator OW.

2. Wyrejestrowanie użytkownika z systemu ochrony wizyjnej może mieć charakter czasowy lub trwały.

§ 15. Trwałe wyrejestrowanie użytkownika z systemu ochrony wizyjnej następuje na wniosek kierownika kom. org. urz. właściwej ds. monitoringu w wyniku:

1) rozwiązania umowy o pracę;
2) ustania lub wygaśnięcia innego stosunku prawnego, na podstawie którego użytkownik miał dostęp do systemu;
3) śmierci użytkownika.

§ 16. Czasowe wyrejestrowanie użytkownika z systemu ochrony wizyjnej następuje na wniosek kierownika kom. org. urz. właściwej ds. monitoringu w wyniku:

1) zwolnienia pracownika z obowiązku świadczenia pracy,
2) zawieszenia w pełnieniu obowiązków służbowych,
3) urlopu,
4) usprawiedliwionej nieobecności w pracy podległego pracownika trwającej nieprzerwanie powyżej 30 dni,

- zgodnie z odrębnymi przepisami.

§ 17 . Wyrejestrowanie następuje przez:

1) zablokowanie konta użytkownika OW do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe);
2) usunięcie danych użytkownika OW z bazy użytkowników systemu OW (wyrejestrowanie trwałe).

§ 18. Po ustaniu przyczyn określonych w §16 następuje przywrócenie poprzednich uprawnień w systemie OW.

§ 19. Jeśli po czasowym wyrejestrowaniu użytkownika OW i po powrocie pracownika do pracy nastąpiła zmiana w zakresie powierzonych mu zadań zakresie ochrony wizyjnej, administrator OW nadaje uprawnienia zgodnie z § 13 ust. 1

Rozdział 3
Metody i środki uwierzytelniania, procedury związane z ich zarządzaniem oraz użytkowaniem

§ 20. Każdy użytkownik systemu ochrony wizyjnej posiada swój unikalny w systemie identyfikator.

§ 21. Dla każdego użytkownika systemu ochrony wizyjnej ustala się odrębne konto zawierające w szczególności: identyfikator, hasło pierwszego logowania, dane o uprawnieniach użytkownika, profil.

§ 22. W systemach OW służących do przetwarzania danych osobowych stosowane jest uwierzytelnianie użytkownika przy pomocy jego identyfikatora lub hasła.

§ 23. W systemie OW stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do systemu operacyjnego oraz dostępu do aplikacji.

§ 24. Hasła tymczasowe do konta użytkownika OW w przypadku utworzenia nowego konta, a także w sytuacjach awaryjnych związanych np.: z zagubieniem, utratą lub zapomnieniem hasła osobistego przez użytkownika OW konta tworzone są, na ustny wniosek użytkownika OW przez administratora OW.

§ 25. Administrator OW, jeżeli system na to pozwala, ustawia wymuszenie zmiany hasła przy pierwszym logowaniu użytkownika OW.

§ 26. Tryb przekazywania hasła tymczasowego, o którym mowa w § 24, odbywa się w sposób zapewniający bezpieczeństwo i poufność przekazywanych informacji, w szczególności w sposób uniemożliwiający innej osobie ich podsłuchanie lub nieuprawnione wykorzystanie.

§ 27. Zakazuje się przekazywania haseł poprzez osoby trzecie lub przy użyciu metod, które nie gwarantują zachowania jego poufności oraz niezaprzeczalnego ustalenia nadawcy i odbiorcy hasła, np.: przez niechronione wiadomości przekazywane elektronicznie.

§ 28. Po otrzymaniu hasła tymczasowego użytkownik OW ma obowiązek niezwłocznego zalogowania się do systemu informatycznego przy użyciu tego hasła oraz jego zmiany na hasło osobiste.

§ 29. Każdy użytkownik OW zarządza swoimi hasłami dla identyfikatora, który używa.

§ 30. Zabronione jest ujawnianie przez użytkownika OW komukolwiek, jakichkolwiek aktualnych lub poprzednich haseł tymczasowych, haseł osobistych lub innych haseł mu powierzonych.

§ 31. Autoryzacja do wszystkich programów przetwarzających dane osobowe opisanych w niniejszej Polityce możliwa jest wyłącznie za pomocą identyfikatora, hasła.

§ 32. 1. Jeżeli do uwierzytelniania użytkowników używa się hasła, jego zmiana musi następować automatycznie, nie rzadziej niż co 30 dni.

2. Hasła nie mogą być łatwe do odgadnięcia, to znaczy:

1) składają się z minimum 8 znaków, w tym z jednego znaku specjalnego, np.: !@#$%^&*;

2) nie mogą przybierać prostych form, np. 12345678, stanislaw, dom99, haslo, Magda8, itp.

3. Hasła mogą być tworzone według łączenia losowych, nieistniejących w popularnych słownikach sylab/słów, np.: mal-tra-laza-#topa.

§ 33. W celu zapewnienia odpowiedniego bezpieczeństwa haseł i innych identyfikatorów pozwalających na autoryzację w programach przetwarzających dane osobowe nie zaleca się stosowania jakichkolwiek programów i systemów umożliwiających zapamiętywanie identyfikatorów i haseł.

§ 34. Dostęp do każdego z profili użytkowników OW ograniczony jest wyłącznie do jednego pracownika OW oraz administratora OW.

§ 35. 1. Hasła administracyjne do systemów informatycznych muszą być składowane w bezpiecznej postaci i zgodnie z odpowiednimi procedurami składowania.

2. Do przechowywania haseł zapisanych na papierze stosuje się wyłącznie koperty niepozwalające na niezauważalny i nieautoryzowany dostęp do składowanych w nich treści. Koperty z hasłami dodatkowo są składowane w miejscu zapewniającym dostęp tylko osobom upoważnionym.

Rozdział 4
Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

§ 36. Ustala się **procedury rozpoczęcia pracy** przez użytkownika systemu OW:

1) przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem OW oraz w trakcie pracy, każdy użytkownik OW jest obowiązany do zwrócenia bacznej uwagi, czy nie wystąpiły objawy, mogące świadczyć o naruszeniu zasad ochrony danych osobowych;

2) rozpoczęcie pracy przez użytkownika OW w systemie OW obejmuje uruchomienie komputera, wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu;

3) użytkownikowi OW nie wolno w czasie uruchamiania systemu operacyjnego odchodzić od stanowiska pracy; jest to dozwolone tylko i wyłącznie zgodnie z procedurą opisującą tryb zawieszenia pracy z systemem, w którym przetwarzane są dane osobowe;

4) użytkownik OW informuje administratora OW o wszelkich nieprawidłowościach w dostępie do

systemu ochrony wizyjnej.

§ 37. Ustala się **procedury zawieszenia pracy** przez użytkownika OW:

1) w przypadku konieczności tymczasowego opuszczenia stanowiska pracy, użytkownik OW zobowiązany jest, w zależności od przewidywanego okresu swojej nieobecności, do aktywowania wygaszacza ekranu, zabezpieczonego hasłem lub do zablokowania dostępu do użytkowanego systemu komputerowego, np. poprzez jednoczesne naciśnięcie klawiszy {Windows + L} lub {Ctrl + Alt + Delete} i potwierdzenia klawiszem ENTER podświetlonej opcji „Zablokuj komputer", lub poprzez wylogowanie się z systemu;
2) krótkotrwałe przerwy w pracy bez opuszczania stanowiska pracy nie wymagają zamykania aplikacji i wylogowania się z systemu.

§ 38. **1. Zakończenie pracy** przez użytkownika OW polega na wybraniu odpowiedniego polecenia systemowego umożliwiającego zamknięcie komputera lub wylogowanie użytkownika z systemu operacyjnego.

2. Zaleca się zamknięcie wszystkich programów i zapisanie wszystkich otwartych plików, wyłączenie wszystkich drukarek i skanerów znajdujących się w pomieszczeniu.

3. Użytkownik OW powinien pozostać przy komputerze do chwili jego wyłączenia lub wylogowania.

§ 39. Ustala się **zasady użytkowania komputerów przenośnych** zawierających dane osobowe:

1) użytkownik OW jest zobowiązany do zachowania szczególnej ostrożności podczas transportu, przechowywania i użytkowania komputera poza obszarem przetwarzania danych osobowych;
2) komputerów przenośnych lub nośników nie wolno pozostawiać bez nadzoru w miejscach publicznych;
3) w czasie podróży należy przewozić komputery przenośne jako bagaż podręczny i w miarę możliwości je maskować;
4) sprzęt użytkowany poza siedzibą urzędu powinien być ubezpieczony;
5) do połączenia z wewnętrznymi systemami informatycznymi należy stosować bezpieczne połączenia;
6) zdalny dostęp do chronionych informacji (danych osobowych) z sieci publicznej możliwy jest wyłącznie po pomyślnej identyfikacji i uwierzytelnieniu oraz zastosowaniu odpowiednich mechanizmów kontroli dostępu;
7) dane osobowe na komputerach przenośnych użytkowanych poza obszarem przetwarzania danych muszą być zabezpieczone hasłem dostępowym.

§ 40. 1. W przypadku utraty lub kradzieży służbowego komputera przenośnego użytkownik OW niezwłocznie powiadamia o tym fakcie bezpośredniego przełożonego lub administratora.

2. Zawiadamiając bezpośredniego przełożonego użytkownik OW podaje okoliczności utraty komputera oraz opis charakteru utraconych danych wraz z podaniem ich znaczenia, w szczególności w należy określić, czy utracone dane miały charakter danych osobowych.

3. W powiadomieniu o kradzieży należy podać imię i nazwisko użytkownika OW, nazwę miejskiej jednostki lub komórki organizacyjnej, stanowisko oraz nazwę konta.

§ 41. Obowiązuje zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone.

Rozdział 5
Procedury przechowywania, wyodrębniania, udostępniania do wykorzystania i niszczenia plików obrazów zdarzeń w miejscach publicznych rejestrowanych przy użyciu środków technicznych.

§ 42. Obrazy zdarzeń w miejscach publicznych - zwane dalej zapisem z monitoringu- przechowywane są na nośnikach danych urządzeń dokonujących automatycznej rejestracji.

§ 43. Zapisy z systemu ochrony wizyjnej są przechowywane przez 30 dni.

§ 44. Zabrania się:

1) rejestrowanie obrazów wyświetlanych na monitorach za pomocą urządzeń przenośnych wszelkiego typu;
2) używania wszelkich nieautoryzowanych przez administratora nośników danych w systemie ochrony wizyjnej;
3) drukowania obrazów wyświetlanych na monitorach (tzw. stopklatek).

§ 45. Wyodrębnienie plików zapisu z systemu ochrony wizyjnej następuje na pisemny lub elektroniczny wniosek podmiotów upoważnionych ustawowo do przetwarzania danych osobowych prowadzących postępowanie w danej sprawie.

§ 46. Właściwym dla wyrażenia zgody na udostępnienie wyodrębnionych plików zapisu z monitoringu jest kierownik kom. org. urz. właściwej ds. monitoringu.

§ 47. Wyodrębnienia plików zapisu z systemu ochrony wizyjnej dokonuje osoba uprawniona.

§ 48. Wyodrębnione pliki zapisu z monitoringu, o którym mowa w § 44 przechowywane są na wyodrębnionym zasobie sieciowym do czasu ich wydania uprawnionemu wnioskodawcy.

§ 49. Nośniki zewnętrzne z wyodrębnionymi plikami zapisu na potrzeby realizacji § 45 przechowywane są w pomieszczeniach centrum monitoringu w sposób gwarantującym zabezpieczenie ich przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.
.

§ 50. 1. Wyodrębnione pliki zapisu z monitoringu są udostępniane do wykorzystania podmiotom wymienionym w §45 na nośniku uniemożliwiającym edycję przekazywanych plików (płyty CD-R, DVD-R, Blue-Ray) lub zabezpieczone przed edycją na nośniku danych dostarczonym przez wnioskodawcę.

2. Wyodrębnione pliki zapisu z monitoringu są zabezpieczone. przed nieuprawnionym dostępem, za pomocą hasła.

§ 51. Wszystkie nośniki informacji, w szczególności wymienne nośniki danych, zawierające informacje wrażliwe, są ewidencjonowane i odpowiednio oznakowane.

§ 52. 1. Czynność udostępniania plików do wykorzystywania odnotowywana jest na pisemnym wniosku podmiotu, o którym mowa w § 45 .

2. Pisemny wniosek podlega rejestracji w podsystemie informatycznym właściwym do obiegu dokumentów urzędu.

3. Odbiór udostępnianych plików kwitowany jest podpisem na pisemnym wniosku o którym mowa w §45 .

§ 53. 1. Niszczenie zapisu z monitoringu, o którym mowa w § 41 realizowane jest automatycznie poprzez nadpisanie plików po upływie zakresów czasów określonych w § 42.

2. Notatkę służbową, ze zniszczenia plików sporządza osoba uprawniona.

3. Notatka sporządzana jest po upływie nie wcześniej niż 30 dni od zakończenia kolejnego kwartału.

§ 54. 1. Niszczenie wyodrębnionych plików zapisu z monitoringu o których mowa w §44 realizowane jest poprzez ich usunięcie, nie wcześnie niż po upływie 30 dni od daty ich wyodrębnienia.

2. Usunięcia plików dokonuje osoba wymieniona w § 46.

Rozdział 6
Sposób zabezpieczenia systemu ochrony wizyjnej przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz wirusami komputerowymi

§ 55. Zabezpieczenia systemu ochrony wizyjnej przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu OW oraz wirusami komputerowymi realizowane jest zastosowanie rozwiązań technicznych zaimplementowanych w systemie OW.

§ 56. W przypadku wykrycia wirusa komputerowego lub innego oprogramowania złośliwego należy niezwłocznie poinformować o tym fakcie administratora OW lub przełożonego.

§ 57. Zabrania się użytkownikom OW wyłączania, blokowania odinstalowywania programów zabezpieczających komputer (skaner antywirusowy, firewall) przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem.

§ 58. Zabronione jest pobieranie oraz instalowanie na komputerach, jakichkolwiek programów służących do przetwarzania danych osobowych.

§ 59. W celu zabezpieczenia systemu ochrony wizyjnej służącego do przetwarzania danych osobowych przed skutkami awarii zasilania w wytypowanych, przez administratora OW, miejscach stosuje się zasilacz bezprzerwowy typu UPS i wydzieloną sieć elektroenergetyczną.

Rozdział 7
Zgłaszanie incydentów

§ 60.1. Przekazywanie zgłoszeń zidentyfikowanych incydentów, w monitorowanym obszarze, naruszenia bezpieczeństwa osób i mienia, porządku publicznego, przestępstwa lub innych zdarzeń następuje przy zastosowaniu udostępnionych środków łączności do służb właściwych ds. bezpieczeństwa i porządku publicznego w celu zapobiegania zdarzeniom i ujęcia/zatrzymania sprawców wykroczeń lub przestępców.

2. Użytkownik OW dokonujący zgłoszenia incydentu ma obowiązek zaznaczenia i opisania w systemie fragmentu materiału wizyjnego z zajściem na podstawie, którego dokonał zgłoszenia incydentu.

3. Użytkownik OW dokonujący zgłoszenia incydentu ma obowiązek dokonać wpisu do rejestru zdarzeń.

4. Działa opisane w § 60 ust. 2 i 3 należy dokonać w okresie nie dłuższym niż 1 godzina od chwili zgłoszenia incydentu.

§ 61 1. Zgłoszeń incydentów, o których mowa w § 60 ust.1 dokonuje użytkownik OW posiadający odpowiednie upoważnienie.

2. Upoważnienie do zgłaszania incydentów nadaje użytkownikowi OW kierownik jednostki.

Rozdział 8
Konserwacja systemu

§ 62. Naprawy, przeglądy i konserwacje systemu ochrony wizyjnej lub składowych systemu, a także wstępne czynności serwisowe dokonywane są na bieżąco, przez uprawnionych przedstawicieli wyspecjalizowanych podmiotów zewnętrznych (firmę informatyczną) na podstawie zawartej z Miastem Zielona Góra umowy bądź przez uprawnionych pracowników komórki IT.

§ 63. W wypadku przekazania sprzętu lub nośników informacji służących do przetwarzania danych osobowych podmiotowi trzeciemu, administrator OW usuwa i zabezpiecza nośniki danych lub kasuje zapisane na nim dane osobowe w sposób, który uniemożliwi ich odtworzenie. Przy przekazaniu zostaną zachowane szczególne warunki ostrożności, w celu zabezpieczenia danych osobowych przed dostępem osób nieuprawnionych.

§ 64. Wykryte podczas przeglądu i konserwacji nieprawidłowości w działaniu sprzętu lub programów służących do przetwarzania danych osobowych niezwłocznie usuwa podmiot określony w §62.

§ 65. Za prawidłowość przeprowadzenia przeglądów i konserwacji podległego systemu ochrony wizyjnej odpowiada administrator OW.

§ 66. Wszelkie prace związane z naprawami i konserwacją systemu ochrony wizyjnej przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.

Rozdział 9
Naruszenie ochrony danych osobowych w systemie ochrony wizyjnej

§ 67. Użytkownik OW zobowiązany jest zawiadomić kierownikowi kom. org. urz. właściwej ds. monitoringu. lub IOD o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu, a w szczególności o:

1) naruszeniu hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzania hasła);
2) częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień;
3) braku dostępu do systemu ochrony wizyjnej lub zmianie zakresu wyznaczonego dostępu do zasobów;
4) wykryciu wirusa komputerowego;
5) zauważeniu elektronicznych śladów próby włamania do systemu ochrony wizyjnej;
6) znacznym spowolnieniu pracy systemu OW;
7) podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe;
8) zmianie położenia sprzętu komputerowego;
9) zauważeniu fizycznych śladów usiłowania lub dokonania włamania do pomieszczeń, zamykanych szaf lub jednostek centralnych (komputerów).

§ 68. Do czasu przybycia na miejsce kierownikowi kom. org. urz. właściwej ds. monitoringu lub IOD:

1) jeżeli istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego zdarzenia, a następnie uwzględnić w działaniu również ustalenie jego przyczyny lub sprawców;
2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia;
3) zaniechać – jeżeli to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę;
4) zastosować się do instrukcji i regulaminów lub dokumentacji aplikacji, jeśli odnoszą się one do zaistniałego przypadku;
5) przygotować opis incydentu;
6) nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia.

§ 69. Kierownik kom. org. urz. właściwej ds. monitoringu. przyjmujący zawiadomienie jest obowiązany niezwłocznie poinformować IOD o naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu.

§ 70. IOD w uzgodnieniu z administratorem OW może zarządzić, w razie potrzeby, odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części.

Rozdział 10
Monitorowanie stosowania polityki, zmiany polityki

§ 71. **1.** Administrator OW monitoruje bieżącą realizację polityki oraz analizuje konieczność jej dostosowania do zmian wynikających z wymagań prawnych, technologicznych czy organizacyjnych.

2. Propozycje zmian niniejszej polityki przygotowuje i przedstawia kierownikowi kom. org. urz. właściwej ds. monitoringu.

§ 72. Administrator OW dba o stałą edukację pracowników w zakresie bezpieczeństwa informacji m. in. z zakresu ochrony danych osobowych, znajomości niniejszej Polityki czy świadomości istnienia problemów bezpieczeństwa.

§ 73. Administrator OW zobowiązany jest do odnotowania awarii systemu ochrony wizyjnej, zauważonych przypadkach naruszenia niniejszej Polityki przez użytkowników OW, a zwłaszcza o przypadkach posługiwania się przez użytkowników OW nieautoryzowanymi programami, nieprzestrzegania zasad używania oprogramowania antywirusowego, niewłaściwego wykorzystania

sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z procedurami ochrony danych osobowych.

Rozdział 11
Przepisy końcowe

§ 74. W sprawach nieokreślonych niniejszą Polityką należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.

§ 75. 1. Każda osoba mającą dostęp do systemu ochrony wizyjnej jest zobowiązana do zapoznania z niniejszą polityką i zobowiązana do jej przestrzegania w zakresie wynikającym z realizowanych zadań.

2. Naruszenie obowiązków wynikających z niniejszej polityki oraz przepisów o ochronie danych osobowych może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym zgodnie z ustawą.

§ 76. Wszelkie wątpliwości dotyczące sposobu interpretacji niniejszej polityki należy rozstrzygać na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.

§ 77. Wykonanie zarządzenia powierza się dyrektorowi Departamentu Bezpieczeństwa i Zarządzania Kryzysowego.

§ 78. Zarządzenie wchodzi w życie z mocą od dnia 08 sierpnia 2018 r. i podlega publikacji w Biuletynie Informacji Publicznej.

PREZYDENT MIASTA

(-)

mgr inż. Janusz Kubicki