

ZARZĄDZENIE NR 3/17

Dyrektora Gminnego Ośrodka Kultury w Kwidzynie
z dnia 10 lutego 2017 roku

**w sprawie wprowadzenia Instrukcji zarządzania systemem informatycznym służącą
do przetwarzania danych osobowych w Gminnym Ośrodku Kultury w Kwidzynie**

Na podstawie Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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 zm.).

zarządzam, co następuje:

§ 1. Wprowadzam do stosowania Instrukcję zarządzania systemem informatycznym służącą do przetwarzania danych osobowych w Gminnym Ośrodku Kultury w Kwidzynie stanowiącą załącznik do niniejszego zarządzenia.

§ 2. Zarządzenie wchodzi w życie z dniem podpisania

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W GMINNYM OŚRODKU KULTURY W KWIDZYNIE

Zgodnie 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 ze zm.).

§ 1. Instrukcja zarządzania w systemie informatycznym, służącym do przetwarzania danych osobowych w Gminnym Ośrodku Kultury w Kwidzynie określa organizację wewnętrzną zarządzania systemami informatycznymi.

§ 2. Ilekroć w „instrukcji” jest mowa o:

- 1) GOK — rozumie się to przez Gminny Ośrodek Kultury w Kwidzynie
- 2) ASI- należy przez to rozumieć Administratora Systemu Informatycznego
- 3) Ustawie — rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zwaną dalej „ustawą”;
- 4) identyfikatorze użytkownika — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
- 5) hasłe — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
- 6) sieci telekomunikacyjnej — rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne (Dz. U. z 2016r. poz.1489, 1579, 1823)
- 7) sieci publicznej — rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 38, (Dz. U. z 2016r. poz. 1489, 1579, 1823) ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne;
- 8) teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej
- 9) rozliczalności — rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

- 10) integralności danych — rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- 11) raporcie — rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
- 12) poufności danych — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
- 13) uwierzytelnianiu — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§ 3. Za przestrzeganie w GOK zapisów „instrukcji” odpowiedzialny jest Administrator Danych lub w drodze pisemnego upoważnienia do tego osoba zwana Administratorem Systemu Informatycznego. Wzór upoważnienia określa załącznik do „Instrukcji zarządzania systemem informatycznym służącymi do przetwarzania danych osobowych w Gminnym Ośrodku Kultury w Kwidzynie” nr 1.

§ 4. ASI jest odpowiedzialny za przestrzeganie zasad bezpieczeństwa przetwarzania danych osobowych w zakresie systemu informatycznego służącego do tego celu. Do obowiązków ASI należy także kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej i systemu informatycznego. Obowiązkiem jest również zabezpieczenie sprzętu komputerowego przed nieuprawnionym dostępem oraz przeprowadzaniem analizy ryzyka uwzględniającej realne zagrożenia dla systemu informatycznego.

§ 5. W związku z tym, że w GOK przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną, oraz uwzględniając kategorie przetwarzanych danych i zagrożenia wprowadza się poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym na poziomie wysokim, a w związku z tym wprowadza się poniższe postanowienia:

1. Obszar, w który są przetwarzane dane, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Przebywanie osób nieuprawnionych w obszarze, w którym są przetwarzane dane, jest dopuszczalne za zgodą Administratora Danych, Administratora Bezpieczeństwa Informacji lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
2. W systemie informatycznym służącym do przetwarzania danych osobowych, przetwarzać dane mogą wyłącznie osoby posiadające aktualne upoważnienie. Użytkownik przetwarzający dane po otrzymaniu upoważnienia oraz loginu i hasła jest zobowiązany niezwłocznie dokonać zmiany hasła oraz zachować je w tajemnicy. Użytkownik jest zobowiązany do zmiany hasła nie rzadziej niż co 30 dni.

3. System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:
 - a) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
 - b) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie zasilacza awaryjnego UPS.
4. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
5. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie wszystkich danych osobowych muszą być tworzone nie rzadziej niż raz na tydzień.
6. Kopie zapasowe:
 - a) przechowywane w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w pomieszczeniu zamkniętym,
 - b) usuwane niezwłocznie po ustaniu ich użyteczności
7. Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych w tym stosuje hasła dostępu do komputera przenośnego oraz do plików, w których przetwarzane są dane osobowe.
8. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
 - a) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
 - b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
 - c) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

§ 6. 1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie- system ten zapewnia odnotowanie:

- a) daty pierwszego wprowadzenia danych do systemu;
- b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;
- c) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
- d) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
- e) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

2. Odnotowanie informacji następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje.

4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

§ 7. Po zakończeniu pracy w systemie informatycznym użytkownik ma obowiązek wylogować się z systemu.

§ 8. Przeglądy techniczne sprzętu informatycznego w GOK dokonywane będą na polecenie ADO lub ABI do ASI, który ma dbać o ich dobry stan techniczny. W przypadku stwierdzenia usterek technicznych ma obowiązek niezwłocznie powiadomić o tym fakcie Administratora Danych.

§ 9. W przypadku stwierdzenia przez ASI uchybień dotyczących przetwarzania danych w GOK powinien o tym fakcie niezwłocznie powiadomić Administratora Danych oraz wprowadzić takie zabezpieczenia i procedury, które w przyszłości wyeliminują takie zdarzenia.

§ 10. W sprawach nieuregulowanych w niniejszej „instrukcji” mają zastosowanie przepisy ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. oraz Rozporządzeniem 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.

.....
Podpis Administrator Systemu Informatycznego

.....
Podpis Administratora Danych

**UPOWAŻNIENIE DLA ADMINISTRATORA SYSTEMU INFORMATYCZNEGO
W GMINNYM OŚRODKU KULTURY W KWIDZYNIE**

Na podstawie §3 Instrukcji zarządzania systemami informatycznymi z dniem

Wyznaczam Administratora Systemu Informatycznego (ASI), powierzając tę funkcję

Pani/Panu.....

Adres zamieszkania

PESEL.....

Legitymując się dowodem osobistym..... wydanego przez

.....

.....

Podpis Administrator Danych

Ja, niżej podpisany/-a, zobowiązuję się do pełnienia obowiązków Administratora Systemu Informatycznego w oparciu o przepisy wewnętrzne obowiązujące w jednostce organizacyjnej, ze szczególnym uwzględnieniem obowiązków przewidzianych w §4 Instrukcji zarządzania systemem informatycznym.

.....

Podpis

Administratora Systemu Informatycznego

Oświadczenie

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam, lub będę miał/-a dostęp w związku z wykonywaniem jakichkolwiek czynności na rzecz Gminnego Ośrodka Kultury w Kwidzynie .

Zobowiązuję się przestrzegać wszelkich procedur obowiązujących w Gminnym Ośrodku Kultury w Kwidzynie dotyczących ochrony danych osobowych – w szczególności określonych w Polityce Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym.

Oświadczam, że zapoznałem/-am się z przepisami dotyczącymi ochrony danych osobowych, w tym z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2016 r. poz. 922 ze zm.), w tym z zasadami odpowiedzialności karnej określonymi w rozdziale 8 wyżej wymienionej ustawy.

.....

Podpis

Administratora Systemu Informatycznego