Uchwała Nr 8/I/2020

Zarządu Międzygminnego Związku Komunikacyjnego z siedzibą w Jastrzębiu-Zdroju z dnia 30 stycznia 2020 roku.

w sprawie : przyjęcia „Instrukcji Zarządzania Systemem Informatycznym" w Międzygminnym Związku Komunikacyjnym z siedzibą w Jastrzębiu-Zdroju

Na podstawie art. 73 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (j.t. Dz. U. z 2019 r. poz. 506) oraz § 18 Statutu Międzygminnego Związku Komunikacyjnego z siedzibą w Jastrzębiu-Zdroju (Dz. Urz. Woj. Kat. z 1991r., nr 7 poz. 115 z późn. zm.)

Zarząd Związku

u c h w a l a:

§ 1

Przyjąć „Instrukcję Zarządzania Systemem Informatycznym" w Międzygminnym Związku Komunikacyjnym z siedzibą w Jastrzębiu-Zdroju zgodnie z załącznikiem nr 1 do niniejszej uchwały.

§ 2

Traci moc uchwała nr 17/IV/2016 z dnia 26 kwietnia 2016 roku w sprawie instrukcji „Polityka Bezpieczeństwa" oraz ustalenia sposobu zarządzania systemem informatycznym służącym do przetwarzania danych osobowych ze zbiorów Międzygminnego Związku Komunikacyjnego z siedzibą w Jastrzębiu-Zdroju.

§ 2

Wykonanie uchwały powierza się Przewodniczącemu Zarządu Związku.

§ 3

Uchwała wchodzi w życie z dniem podjęcia.

PRZEWODNICZĄCY ZARZĄDU MZK
Roman Foksowicz

Bartosz Ostrowski
RADCA PRAWNY
KL 3159

Załącznik nr 1 do Uchwały Zarządu Nr 8/I/2020 z dnia 30.01.2020 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Dnia 30.01.2020 **Międzygminny Związek Komunikacyjny**
z siedzibą w Jastrzębiu Zdroju
wdraża dokument o nazwie „Instrukcja zarządzania systemem informatycznym" zwany dalej „instrukcją".
Zapisy tego dokumentu wchodzą w życie z dniem 30.01.2020

Ilekroć w „instrukcji" jest mowa o:

1) Podmiocie — rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nieposiadający osobowości prawnej, jednostkę budżetową, jednostkę samorządową;
2) Ustawie — rozumie się przez to ustawę z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz. U. z 2018roku poz. 1000, zwaną dalej „ustawą";
3) Rozporządzeniu – rozumie się przez to rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE zwanego RODO;
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) Haśle — 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 23 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.)
7) Sieci publicznej — rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne;
8) Uwierzytelnianiu — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości;
9) Administratorze – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W przypadku niniejszej Instrukcji Administratorem jest: Międzygminny Związek Komunikacyjny w Jastrzębiu Zdroju, 44-335 Jastrzębie-Zdrój, ul. Przemysłowa 1.

§ 1

1. Za przestrzeganie w podmiocie Międzygminny Związek Komunikacyjny z siedzibą w Jastrzębiu Zdroju zapisów „instrukcji" odpowiedzialny jest Administrator.

2. Zasady opisane w niniejszej instrukcji są zgodne z Rozporządzeniem i Ustawą.

§2

W związku z tym, że w podmiocie Międzygminny Związek Komunikacyjny z siedzibą w Jastrzębiu Zdroju 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:

I

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 pod nadzorem wyznaczonej przez Administratora osoby upoważnionej do przetwarzania danych osobowych.

II

1. W systemie informatycznym służącym do przetwarzania danych osobowych, przetwarzać dane mogą wyłącznie osoby posiadające aktualne upoważnienie nadane przez Administratora. Użytkownik przetwarzający dane po otrzymaniu upoważnienia oraz identyfikatora 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. Hasło nadane przez użytkownika musi składać się z co najmniej z 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

2. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator oraz aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia hasłem.

III

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:
1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego:

•poprzez zainstalowanie programu antywirusowego;

•poprzez zainstalowanie zapory sieciowej realizowanej przy pomocy urządzeń typu UTM (wielofunkcyjne zapory sieciowe);

•poprzez zabezpieczenie sieci Wi-Fi odpowiedniej mocy uwierzytelnieniem – WPA2-PSK.

2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie zasilaczy awaryjnych.

IV

1. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.

2. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

3. 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.

4. Kopie zapasowe:

a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w pomieszczeniu zamkniętym Serwerownia zaopatrzonym w system alarmowy;

b) przechowuje się wykorzystując macierze dyskowe lub dodatkowe systemy archiwizacji danych typu NAS pracujących w wewnętrznej lokalnej sieci;

c) usuwa się niezwłocznie po ustaniu ich użyteczności.

V

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. Na dyskach komputera przenośnego nie wolno przechowywać żadnych danych osobowych.

VI

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

1) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;

2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;

3) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez Administratora.

§3

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

§4

W przypadku stwierdzenia przez Inspektora Ochrony Danych uchybień dotyczących przetwarzania danych w podmiocie powinien o tym fakcie niezwłocznie powiadomić Administratora oraz zaproponować wprowadzenie takich zabezpieczeń i procedur, które w przyszłości wyeliminują takie zdarzenia.

§5

W sprawach nieuregulowanych w niniejszej „instrukcji" mają zastosowanie przepisy Rozporządzenia i Ustawy.

PRZEWODNICZĄCY ZARZĄDU MZK
Roman Foksowicz

.....

Podpis Administratora