WÓJT GMINY
MYCIELIN

ZARZĄDZENIE Nr 56/2019
WÓJTA GMINY MYCIELIN
z dnia 9 września 2019r.

w sprawie wprowadzenia „Instrukcji postępowania w przypadku naruszenia bezpieczeństwa ochrony danych osobowych w Urzędzie Gminy Mycielin"

Na podstawie art. 30 ust. 1 i art. 33 ust. 1 i 3 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (tekst jedn. Dz. U. z 2019r., poz. 506 z późn. zm.) w związku z art. 24 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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)

Wójt Gminy Mycielin z a r z ą d z a co następuje:

§ 1

Wprowadza się **„Instrukcję postępowania w przypadku naruszenia bezpieczeństwa ochrony danych osobowych w Urzędzie Gminy Mycielin"** w brzmieniu stanowiącym załącznik do niniejszego zarządzenia.

§ 2

Zobowiązuję wszystkich pracowników do przestrzegania „Instrukcji postępowania w przypadku naruszenia bezpieczeństwa ochrony danych osobowych w Urzędzie Gminy Mycielin".

§ 3

Nadzór nad przestrzeganiem postanowień „Instrukcji postępowania w przypadku naruszenia bezpieczeństwa ochrony danych osobowych w Urzędzie Gminy Mycielin" sprawuje Administrator Danych Osobowych.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT GMINY
Rafał Szelągowski

Załącznik Nr 1
Tabela form naruszeń bezpieczeństwa danych osobowych

Kod naruszenia	Formy naruszeń	Sposób postępowania
A	**Forma naruszenia ochrony danych osobowych przez pracownika zatrudnionego przy przetwarzaniu danych**	
A.1	W zakresie wiedzy:	
A.1.1	Ujawnianie sposobu działania aplikacji i systemu jej zabezpieczeń osobom niepowołanym.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić Administratora Danych.
A.1.2	Ujawnienie informacji o sprzęcie i pozostałej infrastrukturze informatycznej.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić Administratora Danych.
A.2	**W zakresie sprzętu i oprogramowania:**	
A.2.1	Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.	Niezwłocznie zakończyć działanie aplikacji. Sporządzić raport.
A.2.2	Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony.	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Sporządzić raport.
A.2.3	Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych i sieci.	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Niezwłocznie powiadomić Administratora Danych. Sporządzić raport.
A.2.4	Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych przez osoby nie będące pracownikami.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić, jakie czynności zostały przez osoby nieuprawnione wykonane. Przerwać działające programy. Niezwłocznie powiadomić Administratora Danych. Sporządzić raport.
A.2.5	Samodzielne instalowanie jakiegokolwiek oprogramowania.	Pouczyć osobę popełniającą wymienioną czynność, aby jej zaniechała. Wezwać służby informatyczne w celu odinstalowania programów. Sporządzić raport.
A.2.6	Modyfikowanie parametrów systemu i aplikacji.	Pouczyć osobę popełniającą wymienioną czynność, aby jej zaniechała. Sporządzić raport.

A.3	**W zakresie dokumentów i obrazów zawierających dane osobowe:**	
A.3.1	Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru.	Zabezpieczyć dokumenty. Sporządzić raport.
A.3.2	Przechowywanie dokumentów zabezpieczonych w niedostatecznym stopniu przed dostępem osób niepowołanych.	Powiadomić przełożonych. Spowodować poprawienie zabezpieczeń. Sporządzić raport.
A.3.3	Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić przełożonych. Sporządzić raport.
A.3.4	Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią.	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić przełożonych. Sporządzić raport.
A.3.5	Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Jeżeli ujawnione zostały ważne dane. Sporządzić raport.
A.3.6	Sporządzanie kopii danych na nośnikach danych w sytuacjach nieprzewidzianych procedurą.	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonana kopię. Powiadomić Administratora Danych. Sporządzić raport.
A.4	**W zakresie pomieszczeń i infrastruktury służących do przetwarzania danych osobowych:**	
A.4.1	Opuszczanie i pozostawianie bez dozoru niezamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych.	Zabezpieczyć (zamknąć) pomieszczenie. Powiadomić przełożonych. Sporządzić raport.
A.4.2	Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym.	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość. Powiadomić służby informatyczne i Administratora Danych. Sporządzić raport.
A.4.3	Dopuszczanie , aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakichkolwiek urządzeń do sieci komputerowej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji.	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i Administratora Danych. Sporządzić raport.

A.5	**W zakresie pomieszczeń, w których znajdują się komputery centralne i urządzenia sieci:**	
A.5.1	Dopuszczanie lub ignorowanie faktu, że osoby spoza służb informatycznych i telekomunikacyjnych dokonują jakichkolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (hole, korytarze, itp.).	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i Administratora Danych Sporządzić raport.
B	**Zjawiska świadczące o możliwości naruszenia ochrony danych osobowych**	
B.1	Ślady manipulacji przy układach sieci komputerowej lub komputerach.	Powiadomić niezwłocznie Administratora Danych oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.2	Obecność nowych kabli o nieznanym przeznaczeniu i pochodzeniu.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.3	Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.4	Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.5	Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.6	Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
C	**Formy naruszenia ochrony danych osobowych przez obsługę informatyczną w kontaktach z użytkownikiem**	
C.1	Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej.	Powiadomić Administratora Danych. Sporządzić raport.
C.2	Próba nieuzasadnionego przeglądania (modyfikowania) w ramach pomocy technicznej danych osobowych za pomocą aplikacji w bazie danych identyfikatorem i hasłem użytkownika.	Powiadomić Administratora Danych. Sporządzić raport.

WÓJT GMINY
Rafał Szelągowski

Załącznik
do Zarządzenia Nr 56/2019
Wójta Gminy Mycielin
z dnia 9 września 2019r.

INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH W URZĘDZIE GMINY MYCIELIN

§1

Instrukcja określa zasady postępowania wszystkich osób zatrudnionych przy przetwarzaniu danych osobowych w przypadku naruszenia bezpieczeństwa tych danych, zgodnie z „Tabelą form naruszeń bezpieczeństwa danych osobowych", stanowiącą załącznik Nr 1 do niniejszej instrukcji.

§2

Celem instrukcji jest określenie sposobu postępowania, gdy:

1. stwierdzono naruszenie zabezpieczeń danych osobowych.
2. w przypadku danych przetwarzanych w formie tradycyjnej, stan pomieszczeń, szaf, okien, drzwi, dokumentów lub inne zaobserwowane symptomy mogą wskazywać na naruszenie bezpieczeństwa danych osobowych.
3. w przypadku danych przetwarzanych w formie elektronicznej stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu, jakość komunikacji lub inne zaobserwowane symptomy mogą wskazywać na naruszenie bezpieczeństwa danych osobowych.

§3

1. Za naruszenie ochrony systemu informatycznego uważa się w szczególności:
   1) naruszenie lub próbę naruszenia integralności systemu oraz zbioru danych,
   2) nieuprawniony dostęp lub próbę dostępu do systemu lub pomieszczeń (widoczne uszkodzenia bądź naruszenia zabezpieczeń),
   3) nieautoryzowane zniszczenie lub próbę zniszczenia danych zgromadzonych w systemie,
   4) zmianę lub utratę danych zapisanych na kopiach zapasowych lub archiwalnych, dokonaną w sposób nieautoryzowany,
   5) nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu),
   6) inny stan systemu lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu lub po przerwie w pracy z systemem.
2. Instrukcję stosuje się odpowiednio w przypadku stwierdzenia, że stan pomieszczeń i szaf, bądź innych mebli biurowych, w których przechowywana jest dokumentacja lub zawartości tej dokumentacji wzbudzają podejrzenie, że dostęp do nich mogły mieć osoby trzecie.

§4

1. W przypadku stwierdzenia naruszenia zabezpieczeń lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych jest zobowiązany przerwać przetwarzanie danych i niezwłocznie zgłosić ten fakt bezpośredniemu przełożonemu, Administratorowi Danych, a następnie postępować stosownie do podjętej przez niego decyzji.
2. Administrator Danych, w jednostce w której doszło do naruszenia ochrony danych osobowych:
    1) ocenia zastaną sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane, stan urządzeń i zbioru danych o raz identyfikuje wielkość negatywnych następstw naruszenia ochrony danych osobowych,
    2) podejmuje niezbędne działania mające na celu uniemożliwienie dalszego naruszenia zabezpieczenia systemu (odłączenie urządzeń, odłączenie wadliwych urządzeń, zmiana haseł, blokowanie dostępu do sieci telekomunikacyjnej, programów oraz zbiorów danych),
    3) zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia, jak również sprawdza zawartość zbioru danych osobowych,
    4) sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
    5) sprawdza sposób działania programu (w tym również obecność wirusów komputerowych),
    6) ustala charakter i rodzaj naruszenia oraz metody działania osób naruszających zabezpieczenie systemu,
    7) niezwłocznie zapewnia przywrócenie prawidłowego stanu działania systemu, a w przypadku uszkodzenia baz danych, odtwarza je z ostatnich kopii awaryjnych z zachowaniem należytych środków ostrożności,
    8) sprawdza jakość komunikacji w sieci telekomunikacyjnej,
    9) dokonuje analizy stanu systemu wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia oraz poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych.
3. Do czasu przybycia Administratora Danych, użytkownik:
    1) zabezpiecza dostęp do miejsca lub urządzenia przez osoby trzecie,
    2) wstrzymuje pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamia bez koniecznej potrzeby komputerów i innych urządzeń, które w związku z naruszeniem ochrony zostały wstrzymane,
    3) podejmuje, stosownie do zaistniałej sytuacji inne, niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.
4. Zgłoszenie naruszenia zabezpieczeń danych osobowych powinno zawierać:
    1) opisanie systemów naruszenia zabezpieczeń danych osobowych,
    2) określenie sytuacji i czasu, w jakim stwierdzono naruszenie zabezpieczeń danych osobowych,
    3) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia,
    4) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

§ 5

Administrator Danych lub inna upoważniona przez niego osoba podejmuje wszelkie działania mające na celu:

1. minimalizację negatywnych skutków zdarzenia,
2. wyjaśnienie okoliczności zdarzenia,
3. zabezpieczenie dowodów zdarzenia,
4. umożliwienie dalszego bezpiecznego przetwarzania danych.

§ 6

W celu realizacji zadań wynikających z niniejszej instrukcji Administrator Danych lub inna upoważniona przez niego osoba ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:

1. żądania wyjaśnień od pracowników,
2. korzystania z pomocy konsultantów,
3. nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.

§ 7

Polecenia Administratora Danych lub innej upoważnionej przez niego osoby wydawane w celu realizacji zadań wynikających z niniejszej instrukcji są priorytetowe i winny być wykonywane przed innymi poleceniami, zapewniając ochronę danych osobowych.

§ 8

Odmowa udzielenia wyjaśnień lub współpracy z Administratorem Danych lub inną upoważnioną przez niego osobę, traktowana będzie jako naruszenie obowiązków pracowniczych.

§ 9

Administrator Danych po zażegnaniu sytuacji naruszającej bezpieczeństwo danych osobowych opracowuje raport końcowy, w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski, w tym kadrowe, ograniczające możliwość wystąpienia zdarzenia w przyszłości. Wzór raportu stanowi załącznik Nr 2 do niniejszej instrukcji.

§ 10

Nieprzestrzeganie zasad postępowania określonych w niniejszej instrukcji stanowi naruszenie obowiązków pracowniczych i może być przyczyną do odpowiedzialności dyscyplinarnej określonej w Kodeksie Pracy.

§ 11

Jeżeli skutkiem działania określonego w § 10 jest ujawnienie informacji osobie nieupoważnionej, sprawca może zostać pociągnięty do odpowiedzialności karnej wynikającej z przepisów Kodeksu Karnego.

§ 12

Jeżeli skutkiem działania określonego w § 10 jest szkoda, sprawca ponosi odpowiedzialność materialną na warunkach określonych w przepisach Kodeksu Pracy oraz Prawa Cywilnego.

WÓJT GMINY
Rafał Szelągowski

Załącznik Nr 2
Wzór raportu końcowego sporządzonego przez administratora bezpieczeństwa informacji po zażegnaniu sytuacji naruszającej bezpieczeństwo danych osobowych

Raport
o sytuacji naruszenia bezpieczeństwa danych osobowych

Sporządzający raport:
Imię i nazwisko……
Stanowisko (funkcja) ……
Referat, pokój, nr telefonu ……
Kod formy naruszenie ochrony danych ……(wg tabeli)

1) Miejsce, dokładny czas i data naruszenia ochrony danych osobowych (piętro, nr pokoju, godzina, itp.):
   ……
   ……
2) Osoby powodujące naruszenie (które swoim działanie lub zaniechaniem przyczyniły się do naruszenia ochrony danych osobowych):
   ……
   ……
   ……
3) Osoby, które uczestniczyły w zdarzeniu związanym z naruszeniem ochrony danych osobowych:
   ……
   ……
4) Informacje o danych, które zostały lub mogły zostać ujawnione:
   ……
   ……
5) Zabezpieczone materiały lub inne dowody związane z wydarzeniem:
   ……
   ……
6) Krótki opis wydarzenia związanego z naruszeniem ochrony danych osobowych (przebieg zdarzenia, opis zachowania uczestników, podjęte działania):
   ……
   ……
7) Wnioski:
   ……
   ……

…… (miejsce, data i godzina sporządzenia raportu)

…… (podpis sporządzającego raport)

WÓJT GMINY
Rafał Szelągowski