

Zarządzenie Nr 29/2018
Wójta Gminy Grudusk
z dnia 25 maja 2018r.

w sprawie wprowadzenia „Procedury alarmowej”

Na podstawie art. 33 ust. 1; art. 31 i art.33 ust. 1 i 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2018 r., poz. 994 , ze zm.); 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 95/45/WE (ogólne rozporządzenie o ochronie danych osobowych)

oraz § 3 ust.3, § 4 i § 5 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) zarządzam co następuje:

§ 1

W celu pełnej kontroli oraz zapobieganiu możliwym zagrożeniom związanym z ochroną danych osobowych, wprowadza się do użytku w Urzędzie Gminy Grudusk dokument o nazwie

1. „Procedura alarmowa”
2. Załączniki nr 1, nr 2 i nr 3 nie podlegają publikacji

§ 2

Zobowiązuje się pracowników Urzędu Gminy Grudusk do zapoznania się z dokumentami określonymi w § 1.

§ 3

Wykonanie zarządzenia powierza się Inspektorowi Ochrony Danych.

§ 4

Traci moc zarządzenie Nr 40/2015 Wójta Gminy Grudusk z dnia 23 października 2015 roku w sprawie wprowadzenia „Procedury alarmowej” i „Sprawozdania rocznego stanu systemu ochrony danych osobowych” w Urzędzie Gminy Grudusk.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJTA

mgr Jacek Ogłowski

URZĄD GMINY GRUDUSK

PROCEDURA ALARMOWA

Ochrona danych osobowych w
Urzędzie Gminy Grudusk

Spis treści:

1. Wstęp
2. Podstawowe definicje i pojęcia
3. Procedura alarmowa
4. Rejestr uchybień i zagrożeń oraz szczegółowa instrukcja postępowania dla osób posiadających upoważnienie do przetwarzania danych osobowych w Urzędzie Gminy Grudusk
5. Załączniki

1. Wstęp

Administrator Danych Osobowych w Urzędzie Gminy Grudusk w celu pełnej kontroli oraz zapobiegania możliwym zagrożeniom związanym z ochroną danych osobowych wprowadza dokument o nazwie „Procedura Alarmowa”. Zapisy z tego dokumentu obowiązują wszystkich pracowników Urzędu Gminy Grudusk, którzy przetwarzają dane osobowe w systemach informatycznych i w wersji papierowej.

Z niniejszym dokumentem powinni zapoznać się wszyscy pracownicy, a w szczególności:

- kierownicy referatów i pracownicy z samodzielnych stanowisk pracy;
- osoby upoważnione do przetwarzania danych osobowych w zbiorach i bazach danych;
- obsługa informatyczna Urzędu Gminy Grudusk

Niniejsze procedury korespondują z dokumentem „Polityka Bezpieczeństwa”, która została wprowadzona Zarządzeniem Wójta nr 28/2018 z dnia 25 maja 2018 r.

Za rozpowszechnienie dokumentu i umożliwienie zapoznania się z nim przez wszystkich pracowników odpowiedzialny jest Inspektor Ochrony Danych.

Dokument powinien zostać umieszczony w formie elektronicznej, na wewnętrznych zasobach sieciowych Urzędu Gminy Grudusk, do których dostęp posiadają wszyscy pracownicy Urzędu lub na żądanie powinien zostać im przedłożony w formie papierowej.

Podstawa prawna:

1. Rozporządzenie 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 95/45/WE (ogólnerozporządzenie o ochronie danych osobowych)
2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U poz.1000 z 2018 r.)

2. Podstawowe definicje i pojęcia

Uchybienie - świadome lub nieświadome działania zmierzające do zagrożenia, wskutek których może dojść do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych.

Zagrożenie - świadome lub nieświadome działania, wskutek których doszło do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych.

IOD – Inspektor Ochrony Danych

ADO - Administrator Danych Osobowych

Procedura alarmowa-wskazuje na możliwe zagrożenia oraz definiuje „Dziennik Uchybień i Zagrożeń”, związany z niewłaściwym przetwarzaniem danych osobowych lub ich wyciekami. Celem Procedury Alarmowej jest skatalogowanie możliwych uchybień i zagrożeń oraz opisanie procedur działania w przypadku ich wystąpienia, jak i również ograniczenie ich powstania w przyszłości. Integralną częścią Procedury Alarmowej jest „Dziennik Uchybień i Zagrożeń” - (załącznik nr 1), „Protokół Zagrożenia” - (załącznik nr 2), „Protokół Uchybienia” - (załącznik nr 3), prowadzony przez IOD w przypadku stwierdzenia naruszenia ochrony danych osobowych w podmiocie.

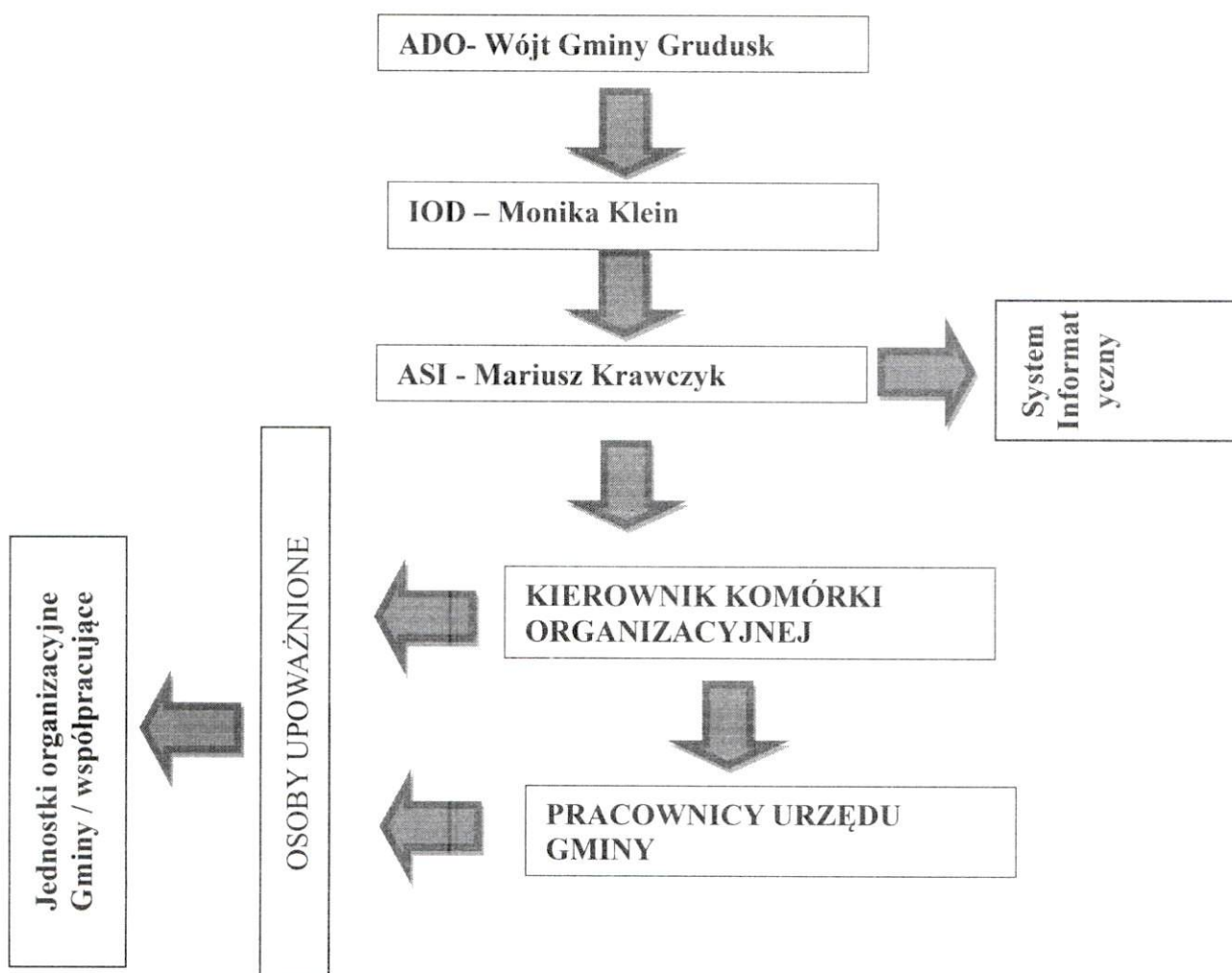
Użytkownik danych- każdy pracownik, który wykonując czynności służbowe, przetwarza dane osobowe, tzn wykonuje na nich operacje takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie

Osoba upoważniona- osoba posiadająca upoważnienie wydane przez ADO lub osobę uprawnioną przez niego i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym w zakresie wskazanym w upoważnieniu

3. Procedura alarmowa

Procedura alarmowa wskazuje na możliwe zagrożenia. Reagowanie w sytuacji powstania uchybień i zagrożenia wiąże się ze strukturą uprawnień oraz z zakresem odpowiedzialności za prawidłowe przetwarzanie danych osobowych w Urzędzie Gminy Grudusk. (rys. 1)

Rys. 1.



4.Rejestr uchybień i zagrożeń oraz szczegółowa instrukcja postępowania dla osób posiadających upoważnienie do przetwarzania danych osobowych w Urzędzie Gminy Grudusk

Do możliwych uchybień i zagrożeń nieświadomych wewnętrznych i zewnętrznych należą działania pracowników Urzędu Gminy Grudusj lub osób nie będących pracownikami Urzędu Gminy, w następstwie których może dojść lub doszło do zniszczenia danych, wycieku danych lub naruszenia ich poufności.

W szczególności są to działania takie jak np.:

- niewłaściwe zabezpieczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe,
- niewłaściwe zabezpieczenie danych przetwarzanych na stanowisku pracy,
- niewłaściwe zabezpieczenie sprzętu komputerowego,
- włamanie do systemu,
- dopuszczenie do przetwarzania danych przez osoby nieposiadające upoważnienia,
- wykorzystywanie sprzętu do celów prywatnych z użyciem nie sprawdzonych nośników danych
- brak reakcji na zagrożenia,
- kradzież danych,
- pozostawienie bez opieki, a w konsekwencji utrata danych,
- działanie wirusów i innego szkodliwego oprogramowania

Do uchybień i zagrożeń umyślnych wewnętrznych i zewnętrznych należą celowe działania pracowników Urzędu Gminy Grudusk, w następstwie których może dojść lub doszło do zniszczenia, wycieku danych lub naruszenia ich poufności.

W szczególności są to działa takie jak np.:

- kradzież sprzętu informatycznego,
- nie stosowanie obowiązujących procedur,
- brak szkolenia w zakresie ochrony danych osobowych,
- niewłaściwe niszczenie dokumentów,
- celowe zniszczenie sprzętu, danych osobowych lub nośników danych

Do uchybień i zagrożeń losowych należą sytuacje losowe, w następstwie których może dojść do zniszczenia danych, wycieku lub naruszenia ich poufności.

W szczególności są sytuacje takie jak np.:

- klęski żywiołowe,
- zalanie wodą,
- pożar,
- awarie serwerów i innych urządzeń wchodzących w skład systemu informatycznego,
- przerwy w dostawie prądu (zasilania),
- niesprawne źródła zasilania awaryjnego

Każdy pracownik Urzędu Gminy Grudusk posiadający upoważnienie do przetwarzania danych osobowych, w przypadku stwierdzenia uchybienia lub zagrożenia ma obowiązek niezwłocznie powiadomić o tym fakcie Inspektora Ochrony Danych lub Administratora Danych.

Inspektor Ochrony Danych w przypadku stwierdzenia uchybienia ma obowiązek:

- odnotować każde uchybienie w dokumencie: „Dziennik Uchybień i Zagrożeń” - załącznik nr 1
- sporządzić dokument: „Protokół Uchybienia” - załącznik nr 3
- wprowadzić procedury uniemożliwiające ponowne powstanie uchybienia

Inspektor Ochrony Danych w przypadku stwierdzenia zagrożenia ma obowiązek:

- zabezpieczyć dowody,
- powiadomić policję (w przypadku włamania),
- zabezpieczyć dane osobowe oraz nośniki danych,
- odnotować każde zagrożenie w dokumencie: „dziennik Uchybień i Zagrożeń” - załącznik nr1,
- sporządzić dokument : „Protokół Zagrożenia” - załącznik nr 2
- wprowadzić procedury uniemożliwiające ponowne powstanie zagrożenia,
- powiadomić o zaistniałej sytuacji Administratora Danych

Administrator Danych w przypadku stwierdzenia zagrożenia może wyciągnąć konsekwencje dyscyplinarne wobec osób odpowiedzialnych za zagrożenie.

Kod uchybienia lub zagrożenia	Uchybienia i zagrożenia nieświadome wewnętrzne i zewnętrzne	Postępowanie
01	Pomieszczenie, w którym przechowywane są dane osobowe pozostaje bez nadzoru	Zabezpieczyć dane osobowe i powiadomić IOD.
02	Komputer nie jest zabezpieczony hasłem	Zabezpieczyć dane osobowe i powiadomić IOD.
03	Dostęp do danych osobowych mają osoby nieposiadające upoważnienia	Uniemożliwić dostęp osób bez upoważnienia i powiadomić IOD
04	Nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym	Powiadomić IOD, który sprawdza system uwierzytelniania
05	Próba kradzieży danych osobowych poprzez zewnętrzny nośnik danych	Powiadomić IOD , który zabezpiecza nośnik danych, powiadomić ADO
06	Próba kradzieży danych osobowych w formie papierowej	Powiadomić IOD, zabezpieczyć dane, powiadomić ADO
07	Nieuprawniony dostęp do danych osobowych w formie papierowej	Powiadomić IOD
08	Dane osobowe przechowywane są w niezabezpieczonym pomieszczeniu	Powiadomić IOD, który zabezpiecza pomieszczenie
09	Próba włamania do pomieszczenia/budynku	Zabezpieczyć dowody, powiadomić IOD, który sprawdza stan uszkodzeń, zabezpiecza dowody i wzywa policję
10	Działanie zewnętrznych aplikacji, wirusów, złośliwego oprogramowania	Należy zrobić audyt systemów zabezpieczeń, a w szczególności systemów antywirusowych, firewall. IOD ocenia czy nie doszło do utraty danych osobowych
11	Brak aktywnego oprogramowania	Powiadomić IOD, który

	antywirusowego	aktualizuje oprogramowanie antywirusowe
12	Zniszczenie lub modyfikacja danych osobowych w formie papierowej	Powiadomić IOD, zabezpieczyć dowody, powiadomić ADO
13	Zniszczenie lub modyfikacja danych osobowych w systemie informatycznym	Powiadomić IOD, zabezpieczyć dowody, powiadomić ADO
14	Uszkodzenie komputerów, nośników danych	Powiadomić ASI, który sprawdza stan uszkodzeń i powiadamia ADO
15	Próba nieuprawnionej interwencji przy sprzęcie komputerowym	Uniemożliwić dostęp osób do sprzętu komputerowego, powiadomić IOD
16	Zdarzenia losowe	Oszacować powstałe straty

Nazwa i adres podmiotu

Miejscowość i data

.....

.....

„Protokół Zagrożenia”

Data i godzina wystąpienia zagrożenia

Kod zagrożenia

Opis zagrożenia

.....
.....
.....
.....
.....

Przyczyny powstania zagrożenia

.....
.....
.....
.....
.....

Zaistniałe skutki zagrożenia

.....
.....
.....
.....
.....

Podjęte działania naprawczo-zapobiegawcze

.....
.....
.....
.....
.....

Inspektor Ochrony Danych

Administrator Danych Osobowych

.....

.....

Podpis

Podpis

Nazwa i adres podmiotu

Miejscowość i data

.....

.....

„Protokół Uchybienia”

Data i godzina wystąpienia uchybienia.....

Kod uchybienia

Opis uchybienia

.....
.....
.....
.....

Przyczyny powstania uchybienia

.....
.....
.....
.....

Zaistniałe skutki uchybienia

.....
.....
.....
.....

Podjęte działania naprawczo-zapobiegawcze

.....
.....
.....
.....

Inspektor Ochrony Danych

Administrator Danych Osobowych

.....

Podpis

.....

Podpis