Zarządzenie Nr 4/2017
Wójta Gminy Udanin
z dnia 26 stycznia 2017 r.

w sprawie powołania Administratora Bezpieczeństwa Informacji i jego zastępcy oraz Administratora Systemu Informatycznego w Urzędzie Gminy Udanin.

Na podstawie art. 33 ust.3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz.U. z 2016 r. poz. 446 ze zm.), art. 36a ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r., poz. 922 ze zm.), zarządzam co następuje:

§ 1

1. Powołuję Pana Piotra Łabędzkiego na **Administratora Bezpieczeństwa Informacji** (ABI) w Urzędzie Gminy Udanin.
2. Zakres zadań i uprawnień Administratora Bezpieczeństwa Informacji stanowi załącznik Nr 1 do niniejszego zarządzenia.
3. W zakresie czynności wynikających z pełnienia funkcji i realizacji zadań związanych z ochroną danych osobowych Administrator Bezpieczeństwa Informacji podlega bezpośrednio Wójtowi Gminy Udanin.

§ 2

1. Powołuję Panią Marię Syniawa na **zastępcę Administratora Bezpieczeństwa Informacji** w Urzędzie Gminy Udanin.
2. Zakres zadań określa załącznik Nr 2 do niniejszego zarządzenia.

§ 3

1. Powołuję Pana Łukasza Skrzypiec na **Administratora Systemu Informatycznego** (ASI) w Urzędzie Gminy Udanin.
2. Zakres obowiązków ASI stanowi załącznik Nr 3 do niniejszego zarządzenia.
3. W czasie nieobecności ASI jego obowiązki przejmuje ABI.

§ 4

Traci moc Zarządzenie Nr 0152/7/2007 Wójta Gminy Udanin z dnia 29 maja 2007 r. w r sprawie powołania Administratora Bezpieczeństwa Informacji w Urzędzie Gminy Udanin i Zarządzenie N0152/18/2009 Wójta Gminy Udanin z dnia 09 października 2009 r. zmieniające zarządzenie w sprawie powołania Administratora Bezpieczeństwa Informacji w Urzędzie Gminy Udanin oraz Zarządzenie Nr 0152/7/2009 Wójta Gminy Udanin z dnia 16 marca 2009 r. w sprawie powołania Administratora Sieci Komputerowej oraz osoby jego zastępującej w Urzędzie Gminy Udanin.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Teresa Olkiewicz

Załącznik Nr 1 do Zarządzenia
Nr 4/2017 Wójta Gminy Udanin
z dnia 26 stycznia 2017 r.

Zakres działania Administratora Bezpieczeństwa Informacji (ABI)

1. Administrator Bezpieczeństwa Informacji – zwany dalej ABI wykonuje zadania w zakresie niniejszego zarządzenia oraz upoważnienia nadanego przez Administratora danych Osobowych.

2. Zadaniem ABI jest realizacja zadań określonych art.36a pkt 2 ustawy z dnia 29 sierpnia 1997 r. (t.j. Dz. U. z 2016 r., poz. 922 ze zm.) – w szczególności do zadań Administratora Bezpieczeństwa Informacji należy:

1) Zapewnienie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
b) nadzór nad opracowaniem i aktualizacją dokumentacji opisującej sposób przetwarzania danych osobowych (m.in. polityka bezpieczeństwa, instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, ewidencja osób upoważnionych, itp.) oraz kontrola nad przestrzeganiem procedur i zasad w niej określonych,
c) zapewnienie kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane – art.38 ustawy,
d) dokumentowanie przypadków naruszania zasad bezpieczeństwa przetwarzania i ochrony danych osobowych w Urzędzie Gminy w Udaninie,
e) przeprowadzanie okresowych kontroli w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarzane są dane osobowe,
f) zapewnienie szkoleń dla pracowników z zakresu przetwarzania i ochrony danych osobowych.
2) Nadzorowanie prowadzenia lokalnego rejestru zbiorów danych osobowych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1 ustawy, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2–4a i 7 ustawy oraz zgodnie z zapisami Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. (Dz. U. 2015 poz. 719) określającego sposób prowadzenia rejestru zbiorów danych.
3) Wykonywanie na polecenie Generalnego Inspektora Ochrony Danych Osobowych (GIODO) sprawdzeń, o których mowa w art. 19b ustawy.
4) Nadzór nad prawidłowością archiwizacji zbiorów danych osobowych przetwarzanych w systemie informatycznym oraz ich usuwania.

3. Wykonując swoje czynności ABI działa w imieniu Administratora Danych i posiada uprawnienia do:
1) wnioskowania o nadanie lub odebranie uprawnień oraz o ograniczenie użytkownikom dostępu do zasobu danych osobowych nie związany bezpośrednio z jego zakresem obowiązków i zadań,
2) udzielania wytycznych dotyczących usuwania nieprawidłowości stwierdzonych w czasie prowadzonych kontroli i dostosowania ochrony danych do stanu zgodnego z przepisami prawa,
3) kontrolowania treści i realizacji umów dotyczących udostępniania lub powierzania danych do przetwarzania osobom lub podmiotom,
4) podejmowanie odpowiednich działań, wspólnie z ASI, w przypadku wykrycia naruszeń bezpieczeństwa.

4. ABI realizując swoje zadania, współpracuje z kierownikami komórek organizacyjnych oraz ma obowiązek ściśle współpracować z ASI w zakresie przetwarzania danych osobowych w systemach informatycznych.

Załącznik Nr 2 do Zarządzenia
Nr 4/2017 Wójta Gminy Udanin
z dnia 26 stycznia 2017 r

Zakres zadań zastępcy Administratora Bezpieczeństwa Informacji

Do obowiązków zastępcy ABI w szczególności należy:

1) przygotowywanie sprawozdań dla Administratora Danych w zakresie zgodności przetwarzania z przepisami zgodnie z art. 36c ustawy oraz z zapisami Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. (Dz. U. 2015 poz. 745);

2) zapoznanie osób upoważnionych (pracowników, współpracowników Urzędu Gminy, stażystów, itp.) do przetwarzania danych osobowych z przepisami i zasadami ochrony danych osobowych oraz informowanie o zagrożeniach związanych z ich przetwarzanie;

3) zapewnienie złożenia przez pracowników oświadczenia o znajomości przepisów o ochronie danych osobowych oraz zobowiązania do zachowania w tajemnicy danych osobowych oraz informacji na temat zabezpieczania danych osobowych,

4) przygotowywanie upoważnień dla osób dopuszczonych do przetwarzania danych osobowych,

5) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych, zgodnie z wymogami ustawy,

6) weryfikacja zgłoszonych wniosków o wpisanie nowopowstałego zbioru do rejestru zbiorów danych oraz zgłoszeń zmian do zbiorów już zarejestrowanych,

7) zgłaszanie zbiorów danych do rejestracji lub ich zmian w Biurze GIODO - w przypadku zbiorów zawierających dane sensytywne, o których mowa w art. 27 ust.1 ustawy,

8) prowadzenie i aktualizowanie dokumentacji opisującej zastosowaną ochronę, sposób przetwarzania danych w Urzędzie Gminy, a w szczególności:

a) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,

b) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,

c) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,

d) sposób przepływu danych pomiędzy poszczególnymi systemami,

e) ewidencję osób upoważnionych do przetwarzania danych osobowych w Urzędzie Gminy.

9) prowadzenie lokalnego rejestru zbiorów danych osobowych, o których mowa w art. 36a ust.2 pkt 2 ustawy oraz zgodnie z zapisami Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. określającego sposób prowadzenia rejestru zbiorów danych.

Załącznik Nr 3 do Zarządzenia
Nr 4/2017 Wójta Gminy Udanin
z dnia 26 stycznia 2017 r.

Zakres działania Administratora Systemu Informatycznego (ASI)

Administrator Systemu Informatycznego w zakresie zadań wykonywanych dla zapewnienia systemom informatycznym bezpieczeństwa, współpracuje bezpośrednio z Administratorem Bezpieczeństwa Informacji (ABI.

Do obowiązków Administratora Systemu Informatycznego należy:

1) zapewnienie optymalnej ciągłości działania systemu informatycznego (awaryjne zasilanie komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych) oraz utrzymanie systemu w należytej sprawności technicznej,

2) sprawowanie nadzoru nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych osobowych za pośrednictwem urządzeń teletransmisji,

3) przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych oraz podejmowanie odpowiednich działań zabezpieczających stan systemu informatycznego w urzędzie w przypadku wykrycia naruszenia bądź podejrzenia naruszenia zabezpieczeń, m.in. identyfikowanie i analizowanie zagrożeń, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych Urzędu,

4) monitorowanie działania zabezpieczeń wdrożonych w systemach informatycznych oraz zgłaszanie potrzeb w zakresie zmiany w konfiguracji sprzętu lub oprogramowania mające wpływ na bezpieczeństwo systemu komputerowego,

5) zgłaszanie potrzeb zakupu systemów operacyjnych, oprogramowania antywirusowego oraz systemów kryptograficznych podnoszących bezpieczeństwo danych osobowych, gwarantujących spełnienie wymogów określonych ustawą,

6) zakup urządzeń i nośników umożliwiających wykonywanie kopii zapasowych danych osobowych w systemach informatycznych,

7) nadzór nad naprawami, likwidacją urządzeń komputerowych, na których zapisane są dane osobowe oraz nad wykonywaniem czynności serwisowych przez podmiot zewnętrzny w systemach informatycznych w celu wyeliminowania:

a) możliwości wykonywania kopii danych osobowych przez osoby nieupoważnione,

b) przemieszczania urządzeń komputerowych i ich części służących do przetwarzania danych osobowych poza obszar objęty ochroną,

c) podmiany elementów sprzętu komputerowego lub oprogramowania na inny, który zawiera cechy ukryte,

8) aktualizacja systemów informatycznych oraz wykonywanie okresowych przeglądów i konserwacji - zgodnie z odrębnymi procedurami - sprzętu IT, systemów informatycznych, aplikacji oraz elektronicznych nośników informacji, na których zapisane są dane osobowe,

9) sprawowanie kontroli przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontroli działań inicjowanych z sieci publicznej a systemem informatycznym,

10) realizacja decyzji Administratora Danych lub ABI odnośnie nadania osobom uprawnień dostępu do danych i wybranych funkcji narzędzi służących do ich przetwarzania, jak (rejestrowanie i wyrejestrowywanie użytkowników, dokonywanie modyfikacji uprawnień w systemie), m.in.:

a) tworzenie kont użytkowników w systemach informatycznych,
b) przypisywanie do kont, startowych haseł uwierzytelniających użytkowników tych kont,
c) przypisywanie do założonych kont polityk odnośnie jakości haseł i częstotliwości ich zmiany,
d) resetowanie utraconych haseł,
e) usuwanie kont i uprawnień dla kont osób, które zakończyły pracę w Urzędzie,

11) utrzymanie w sprawności system alarmowy w budynku Urzędu, w tym prowadzenie ewidencji z dokonanych napraw i czynności konserwacyjnych urządzeń i instalacji,

12) monitorowanie legalności oprogramowania wykorzystywanego na stacjach roboczych,

13) zapewnienie serwerom i stacjom roboczym niezbędnych licencji programowych,

14) zapewnienie eksploatowanym systemom opieki serwisowej producenta – zawieranie umów regulujących formy tej opieki,

15) zatwierdzanie wniosków zgłoszeń do rejestracji zbiorów danych osobowych, w części E i F,

16) wykonywanie i zarządzanie kopiami awaryjnymi oprogramowania systemowego i sieciowego.

17) monitorowanie stanu środowiska IT, stanu sprzętu, wykorzystywanego oprogramowania oraz aktywności sieciowej użytkowników.

18) wykonywanie zadań związanych z tworzeniem kopii zapasowych oprogramowania i danych.

19) prowadzenie ewidencji sprzętu komputerowego.