ZARZĄDZENIE NR 68

WÓJTA GMINY DAMNICA

z dnia 22 marca 2019 r.

w sprawie wyznaczenia Administratora Systemu Informatycznego w Urzędzie Gminy Damnica

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (tekst jednolity: Dz. U. z 2017 r. poz. 1875 z późn. zm.[1)]) w związku z art. 24 ust. 1 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 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z dnia 4 maja 2016 r.)

zarządza się, co następuje:

§ 1. Z dniem 22 marca 2019 r. wyznacza się Pana Łukasza Śmielaka na Administratora Systemu Informatycznego w Urzędzie Gminy Damnica.

§ 2. Zadania Administratora Systemu Informatycznego określa załącznik nr 1 do Zarządzenia.

§ 3. Nadzór nad wykonaniem zarządzenia powierza się Sekretarzowi Gminy Damnica.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
mgr Andrzej Kordylas

[1)] Zmiany tekstu jednolitego zostały ogłoszone w Dz. U. z: 2017 r. poz. 2232; 2018 r. poz. 130.

Uzasadnienie
do Zarządzenia nr 68
Wójta Gminy Damnica
z dnia 22 marca 2019 r.

W myśl art. 24 ust.1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 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) (Dz. Urz. UE L 119 z dnia 4 maja 2016 r.), uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Wyznaczenie ASI to rozwiązanie organizacyjne mające na celu nadzorowanie i realizowanie zasad bezpieczeństwa przetwarzania i ochrony danych osobowych w systemach informatycznych Urzędu Gminy w Damnicy.

INSPEKTOR
mgr inż. Zdzisław Kołtuniak

Załącznik do Zarządzenia Nr 68
Wójta Gminy Damnica
z dnia 22 marca 2019 r.
w sprawie wyznaczenia
Administratora Systemów Informatycznych
w Urzędzie Gminy Damnica

Zakres zadań i uprawnień Administratora Systemów Informatycznych W Urzędzie Gminy Damnica

1. Administrator Systemów Informatycznych, zwany dalej ASI, wykonuje zadania w zakresie niniejszego Zarządzenia, polityk, instrukcji oraz upoważnień nadanych przez Administratora Danych Osobowych.
2. Celem działania ASI jest nadzorowanie i realizowanie zasad bezpieczeństwa przetwarzania i ochrony danych osobowych w systemach informatycznych Urzędu Gminy Damnica.
3. Zadaniem ASI jest współpraca z Inspektorem Ochrony Danych Osobowych w zakresie kontroli nad przestrzeganiem zasad ochrony danych osobowych pod kątem zabezpieczeń teleinformatycznych.
4. Administrator Systemów Informatycznych odpowiedzialny jest za:
1) bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego, w tym zabezpieczenie zbiorów danych oraz programów służących do przetwarzania danych osobowych poprzez systematyczne wykonywanie kopii zapasowych,
2) optymalizację wydajności systemu informatycznego, instalacje i konfiguracje sprzętu sieciowego i serwerowego,
3) instalacje i konfiguracje oprogramowania systemowego, sieciowego,
4) przegląd systemów informatycznych w celu określania ich poziomu sprawności, biorąc pod uwagę racjonalne wykorzystanie sprzętu oraz bezpieczeństwo danych przetwarzanych z jego wykorzystaniem,
5) konfigurację i administrowanie oprogramowaniem systemowym i sieciowym, a w tym:
- kontrolę dostępu (rejestrowanie i wyrejestrowywanie użytkowników, zarządzanie hasłami, użycie uprzywilejowanych programów narzędziowych),
- środki ochrony kryptograficznej (polityka stosowania zabezpieczeń, zarządzanie kluczami),
- bezpieczeństwo fizyczne i środowiskowe oraz bezpieczeństwo eksploatacji (zarządzanie zmianami, zarządzanie pojemnością, zapewnienie ciągłości działania, rejestrowanie zdarzeń i monitorowanie),

- bezpieczeństwo komunikacji (zabezpieczenie, rozdzielenie sieci),
- ochronę przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem,

6) monitorowanie przestrzegania RODO, a w tym działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,

7) współpracę z IOD podczas przeprowadzania procesu analizy ryzyka wśród obszarów lub też zasobów, które nie są zabezpieczone lub zastosowane wobec nich zabezpieczenia nie są wystarczające,

8) nadzór nad zapewnieniem awaryjnego źródła zasilania oraz zabezpieczenie przed zakłóceniami w sieci zasilającej systemów informatycznych służących do przetwarzania danych osobowych, których nagła przerwa w pracy mogłaby spowodować utratę danych lub naruszenie ich integralności.

9) współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,

10) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,

11) zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie,

12) przechowywanie kopii w miejscu zabezpieczającym je przed nieuprawnionym dostępem , modyfikacją, uszkodzeniem lub zniszczeniem.

13) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji i zarządzanie incydentami związanymi z bezpieczeństwem informacji,

14) wyjaśnianie i dokumentowanie, wspólnie z IOD, przypadków naruszenia zasad bezpieczeństwa systemów informatycznych

15) kontrolowania, wspólnie z IOD, pracowników w zakresie przestrzegania zasad bezpieczeństwa i ochrony danych osobowych poprzez prowadzone sprawdzenia (kontrole lub audyty).

16) nadzór nad naprawą oraz likwidacją urządzeń komputerowych tj. urządzeniami, dyskami lub innymi elektronicznymi nośnikami informacji, zawierającymi dane osobowe, przeznaczonymi do likwidacji, naprawy lub do przekazania podmiotowi nieuprawnionemu do przetwarzania danych administratora (pozbawienie danych, w sposób uniemożliwiający ich odzyskanie),

17) realizację wniosków Sekretarza Gminy o nadanie, modyfikację, odebranie uprawnień w systemach informatycznych,

18) weryfikację upoważnień do przetwarzania danych osobowych lub innej podstawy prawnej pozwalającej na przydzielenie uprawnień,

19) rejestrowanie uprawnień użytkownika w systemie informatycznym,

20) tymczasowe zawieszanie uprawnień w przypadku powzięcia informacji o długotrwałej nieobecności pracownika trwającej dłużej niż 60 dni,

21) wnioskowanie do Administratora Danych Osobowych lub Inspektora Ochrony Danych w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń,

22) zarządzanie licencjami, procedurami ich dotyczącymi.

23) bieżący nadzór, wspólnie z Inspektorem Ochrony Danych Osobowych, nad wypełnianiem zaleceń Systemu Zarządzania Bezpieczeństwem Informacji oraz przestrzeganiem Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

WÓJT

mgr Andrzej Kordylas