ZARZĄDZENIE NR 29/2016
Wójta Gminy Działdowo

z dnia 11 marca 2016 r.

w sprawie Polityki Bezpieczeństwa Danych Osobowych
w Urzędzie Gminy w Działdowie

Na podstawie art. 31 i 33 ust. 3 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (Dz. U. z 2015r., poz. 1515 z późn. zm.), art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2015r. poz. 2135 z późn. zm.) oraz § 3, 4 i 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004r., Nr 100, poz. 1024) – zarządzam, co następuje:

§ 1. Wprowadzam i wdrażam do stosowania „Politykę Bezpieczeństwa w Zakresie Przetwarzania Danych Osobowych", stanowiącą załącznik Nr 1 do niniejszego zarządzenia, „Instrukcję Zarządzania Systemem Informatycznym", stanowiącą załącznik Nr 2 do niniejszego zarządzenia, oraz "Instrukcję Postępowania w Sytuacji Naruszenia Systemu Ochrony Danych Osobowych„, stanowiącą załącznik Nr 3 do niniejszego zarządzenia.

§ 2. Do przestrzegania przepisów, o których mowa w § 1 zobowiązuje się:

1) wszystkich pracowników, którzy zostali upoważnieni do przetwarzania danych osobowych,
2) pracowników przebywających w pomieszczeniach biurowych tworzących obszar, w którym przetwarzane są dane osobowe,
3) kierowników jednostek organizacyjnych korzystających z zasobów informatycznych Urzędu Gminy Działdowo.

§ 3. Wykonanie zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji oraz Administratorowi Systemu.

§ 4. Traci moc Zarządzenie nr 47/2006 Wójta Gminy Działdowo z dnia 09 maja 2006 r.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik NR 1 do Zarządzenia Nr 29/2016

Wójta Gminy Działdowo

z dnia 11 marca 2016 r.

POLITYKA BEZPIECZEŃSTWA W ZAKRESIE PRZETWARZANIA DANYCH OSOSBOWYCH.

§ 1. Celem Polityki Bezpieczeństwa danych osobowych, zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych w zakresie ochrony danych osobowych sposobu przetwarzania w Urzędzie Gminy Działdowo informacji zawierających dane osobowe.

§ 2. Określenia użyte w Polityce Bezpieczeństwa należy rozumieć zgodnie z ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2015r. poz. 2135 z późn. zm.), a ponadto inne oznaczają:

1. Urząd – Urząd Gminy w Działdowie,

2. Administrator Danych - Gmina Działdowo reprezentowana przez Wójta Gminy Działdowo,

3. Komórka organizacyjna – odpowiednio komórki organizacyjne, o których mowa w „Regulaminie Organizacyjnym Urzędu Gminy Działdowo”

4. Użytkownik – osoba upoważniona do przetwarzania danych osobowych,

5. Administrator Systemu – osoba upoważniona do zarządzania systemem informatycznym,

6. Zabezpieczenie systemu informatycznego – należy przez to rozumieć wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych a także ich utratą.

§ 3. Utrzymanie bezpieczeństwa przetwarzanych przez Urząd danych osobowych rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie.

§ 4. Politykę Bezpieczeństwa stosuje się do wszystkich danych osobowych przetwarzanych w urzędzie.

§ 5. 1. W systemie informacyjnym urzędu przetwarzane są informacje służące do wykonywania zadań z zakresu administracji publicznej.

2. Informacje te są przetwarzane i składowane zarówno w postaci papierowej jak i elektronicznej.

3. Na pomieszczenia przetwarzania danych osobowych składają się pomieszczenia biurowe oraz części pomieszczeń, gdzie Administrator Danych prowadzi działalność, są to:

1) Serwerownia;

2) Pomieszczenia biurowe, w których zlokalizowane są stacje robocze;

3) Pomieszczenia, w których przechowywane są sprawne oraz uszkodzone elektroniczne nośniki informacji, kopie zapasowe;

4) Pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego;

5) Pomieszczenia, w których zlokalizowane są zbiory nieinformatyczne.

§ 6. 1. Przebywanie wewnątrz obszarów, o których mowa w **§ 5** ust. 3, osób nieuprawnionych do przetwarzania danych osobowych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych lub za jej zgodą.

2. Budynki lub pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane podczas nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób ograniczający możliwość dostępu do nich osobom nieupoważnionym.

§ 7. Każdorazowe naruszenie zasad ochrony danych osobowych powinno być zgłaszane do Administratora Bezpieczeństwa Informacji.

§ 8. Do stosowania zasad określonych w Polityce Bezpieczeństwa zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy, stażyści oraz inne osoby mające dostęp do informacji podlegających ochronie.

§ 9. Niniejsza Polityka Bezpieczeństwa w zakresie przetwarzania danych osobowych ustanawia metody zarządzania oraz wymagania niezbędne do zapewnienia skutecznej i spójnej ochrony przetwarzanych danych osobowych.

§ 10. Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w urzędzie zasad ochrony danych osobowych oraz otrzymują stosowne upoważnienie.

§ 11. Zakres czynności dla osoby dopuszczonej do przetwarzania danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę danych osobowych w stopniu odpowiednim do zadań tej osoby realizowanych przy przetwarzaniu tych danych.

§ 12. Udostępnianie danych osobowych podmiotom upoważnionym do ich otrzymania, na podstawie przepisów prawa, powinno odbywać się wg określonych odrębnymi przepisami procedur postępowania.

§ 13. 1. Za bezpieczeństwo danych osobowych Urzędu , odpowiadają:

1) Administrator Danych,

2) Administrator Bezpieczeństwa Informacji,

3) Administrator Systemu.

2. Administrator Bezpieczeństwa Informacji prowadzi ewidencje:

1) rejestr zbiorów danych osobowych Urzędu (przetwarzanych metodą tradycyjną lub w systemach informatycznych) - załącznik nr 1;

2) ewidencję miejsc i baz danych przetwarzania danych osobowych w systemach informatycznych i sposobu ich zabezpieczania - załącznik nr 2.

3. O ustaniu stosunku pracy z osobą zatrudnioną w urzędzie, stanowisko ds. kadr powiadamia Administratora Bezpieczeństwa Informacji.

§ 14. 1. Obowiązki wynikające z ustawy o ochronie danych osobowych Wójt Gminy Działdowo powierza kierownikom komórek organizacyjnych w zakresie podległych im pracowników, z obowiązkiem współdziałania z Administratorem Bezpieczeństwa Informacji w zakresie swoich właściwości.

2. Kierownicy komórek organizacyjnych urzędu odpowiadają za realizację wymagań obowiązujących przepisów prawa w zakresie ochrony danych osobowych prze osoby bezpośrednio im podległe.

3. Kierownicy komórek organizacyjnych urzędu zobowiązani są do zapoznania podległych pracowników z treścią ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Polityką Bezpieczeństwa w zakresie przetwarzania danych osobowych, Instrukcją zarządzania systemami informatycznymi w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych oraz Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych.

§ 15. Ochrona zasobów danych osobowych urzędu jako całości przed ich nieuprawnionym użyciem lub zniszczeniem jest jednym z podstawowych obowiązków pracowników urzędu .

§ 16. Za bezpieczeństwo informacji odpowiedzialny jest każdy pracownik urzędu .

§ 17. Administrator bezpieczeństwa informacji w Urzędzie Gminy w Działdowie:

1) odpowiada za realizację ustawy o ochronie danych osobowych w zakresie dotyczącym Administratora Bezpieczeństwa Informacji,

2) identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w sposób papierowy i w systemach informatycznych urzędu ,

3) określa potrzeby w zakresie zabezpieczenia zbiorów danych osobowych i systemów informatycznych, w których przetwarzane są dane osobowe.

§ 18. Kierownicy komórek organizacyjnych zobowiązani są do przestrzegania wszystkich przepisów ustawy o ochronie danych, w szczególności poprzez:

1) określanie indywidualnych obowiązków i odpowiedzialności osób zatrudnionych przy przetwarzaniu danych osobowych, wynikających z ustawy o ochronie danych osobowych,

2) wykonywania zaleceń Administratora Bezpieczeństwa Informacji urzędu w zakresie ochrony danych osobowych,

3) wdrażanie, nadzorowanie oraz stwarzanie warunków organizacyjnych i technicznych zapewniających przestrzeganie Polityki Bezpieczeństwa Danych Osobowych w swoich komórkach organizacyjnych,

4) odpowiedzialność za poprawność merytoryczną danych gromadzonych w systemach informatycznych.

§ 19. Administrator Systemu odpowiedzialny jest za:

1) bieżący monitoring, zapewnienie ciągłości działania i optymalizację wydajności systemu informatycznego oraz baz danych,

2) instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego w sposób zabezpieczający dane chronione przed nieupoważnionym dostępem,

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

4) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego i bazodanowego.

5) przeciwdziałanie próbom naruszenia przetwarzanych danych osobowych w systemach informatycznych,

6) zarządzanie licencjami i procedurami ich dotyczącymi oraz prowadzenie profilaktyki antywirusowej.

§ 20. Systemy informatyczne, służące do przetwarzania danych osobowych, muszą spełniać wymogi obowiązujących aktów prawnych regulujących zasady gromadzenia i przetwarzania danych osobowych.

§ 21. Do tworzenia kopii bezpieczeństwa danych osobowych w postaci elektronicznej służą indywidualne systemy archiwizowania dla poszczególnych systemów przetwarzania.

§ 22. Kopie bezpieczeństwa oraz dokumenty papierowe zawierające dane osobowe przechowuje się w warunkach uniemożliwiających dostęp do nich osobom nieuprawnionym.

§ 23. Zasady archiwizacji i brakowania dokumentów reguluje Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. Nr 14, poz.67 z późn. zm.).