ZARZĄDZENIE NR 80/2011
WÓJTA GMINY WODZISŁAW
z dnia 30 grudnia 2011 roku

w sprawie: wprowadzenia regulaminu o ochronie danych osobowych w Urzędzie Gminy w Wodzisławiu

Na podstawie ustawy z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych* (Dz. U. z 2002 r. nr 101, poz. 926 z późn. zm.), ustawy z dnia 26 czerwca 1974 r. *Kodeks Pracy* (Dz. U. z 1998 r. nr 21, poz. 94 z późn. zm.) oraz rozporządzenia Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. *w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika* (Dz. U. z 1996 r. nr 62, poz. 286 z późn. zm.) wprowadza się do stosowania regulamin:

OCHRONA DANYCH OSOBOWYCH

§ 1

Niniejszy dokument określa:
1. zasady postępowania przy przetwarzaniu danych osobowych,
2. prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych.

§ 2

Dane osobowe mogą być przechowywane:
1. w systemach informatycznych,
2. w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych.

§ 3

Przetwarzanie danych osobowych jest możliwe tylko wtedy, gdy uzasadniają to:
1. dobro publiczne,
2. dobro osoby, której dane dotyczą,
3. dobro osób trzecich.

§ 4

1. Każdy z pracowników ma prawo do ochrony dotyczących go danych osobowych.
2. Przetwarzanie danych osobowych może mieć miejsce ze względu na dobro publiczne, dobro osoby, której dane dotyczą, lub dobro osób trzecich w zakresie i trybie określonym regulaminem.
3. Za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

§ 5

1. Administratorem danych osobowych w jednostce jest kierownik jednostki.
2. Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były:
   - przetwarzane w zakresie niezbędnym do wykonywanych zadań powierzonych pracownikom,
   - przetwarzane zgodnie z prawem,
   - merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
   - przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

3. Przetwarzanie danych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą.
4. Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 6

1. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.
2. Wszyscy pracownicy, którzy będą gromadzić i przetwarzać dane osobowe zobowiązani są do bezwzględnego przestrzegania przepisów ustawy przywołanej we wstępie oraz niniejszego regulaminu.
3. Osoby mające upoważnienie do ręcznego i informatycznego przetwarzania danych osobowych zobowiązane są do zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem.
4. Upoważnienia, o których mowa w pkt. 1, są imienne i udzielane w formie pisemnej na czas określony lub na czas nieokreślony – do odwołania udzielonego upoważnienia.
5. Każde upoważnienie jest rejestrowane w rejestrze upoważnień oraz przechowywane w aktach osobowych pracownika.
6. Administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.
7. Administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać:
   - imię i nazwisko osoby upoważnionej,
   - datę nadania i ustania
   - zakres upoważnienia do przetwarzania danych osobowych.
8. Pracownicy, którzy zostali upoważnienie do przetwarzania danych, są obowiązani zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.
9. Administrator danych określa hasła użytkowania komputerów dla przetwarzania danych osobowych.

10. Na stanowiskach, na których przetwarzane są dane osobowe ekrany monitorów powinny być tak ustawione, aby osoby nieupoważnione nie miały dostępu do informacji na nich wyświetlanych.
11. Uruchomienie komputera powinno być za pomocą odpowiedniego hasła,
12. Należy upewnić się, że osoby nieupoważnione nie mają możliwości wglądu do danych,
13. W razie przerwania pracy zastosowanie nieaktywności użytkownika (wygaszacz ekranu), należy upewnić się czy dane zostały zarejestrowane, aby uniknąć utraty danych.
14. Podczas nieobecności osób zatrudnionych przy informatycznym przetwarzaniu danych osobowych pomieszczenia, w których są przetwarzane dane, nie mogą być udostępniane osobom postronnym bez zgody Administratora danych.
15. Zakończenie pracy związanej z przetwarzaniem danych osobowych powinno odpowiadać wszystkim regułom bezpieczeństwa informacji.
16. Kopie informatyczne, wydruki wykonuje się w miarę potrzeb i przechowuje w sposób określony przepisami.
17. Kopie awaryjne przechowuje się zgodnie z prawem, a okresowo sprawdza się pod kątem przydatności.
18. Nośniki danych oraz wydruki, które nie są przeznaczone do udostępniania, przechowuje się w zamykanej szafie, do której dostęp mają tylko osoby uprawnione.
19. Administrator danych sprawdza stan urządzeń, zawartość zbiorów danych osobowych i wielkość ich naruszenia.
20. Dane uzupełnia się w oparciu o kopie awaryjne.

§ 7

1. Pracownikowi zatrudnionemu przy przetwarzaniu danych osobowych w systemie informatycznym administratora bezpieczeństwa informacji przydziela się odrębny identyfikator i hasło.
2. Identyfikator powinien być wpisany do ewidencji pracowników zatrudnionych przy przetwarzaniu danych osobowych.
3. Ustalony identyfikator pracownika nie podlega zmianie w okresie jego zatrudnienia, a po wykreśleniu użytkownika z systemu informatycznego nie może być przydzielony innemu pracownikowi.
4. Hasło powinno zawierać od 5 do 10 znaków, w tym litery duże i małe oraz znaki specjalne i cyfry.
5. Hasło przydzielone pracownikowi zatrudnionemu przy przetwarzaniu danych osobowych pracownik powinien utrzymać w tajemnicy, także po upływie jego ważności.
6. Bezpośredni dostęp do systemu informatycznego zawierającego dane osobowe może nastąpić wyłącznie po podaniu identyfikatora i hasła.
7. Identyfikator osoby, która utraciła uprawnienia dostępu do systemu informatycznego zawierającego dane osobowe, należy natychmiast wyrejestrować z systemu i unieważnić jej hasło.

§ 8

1. Pracownik zatrudniony przy przetwarzaniu danych osobowych w systemie informatycznym obowiązany jest niezwłocznie powiadomić administratora bezpieczeństwa informacji gdy:
   - stwierdzi naruszenie zabezpieczenia systemu informatycznego,
   - stan urządzeń, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakości komunikacji sieci mogą wskazywać na naruszenie zabezpieczeń tych danych.

2. Administrator bezpieczeństwa informacji po stwierdzeniu naruszenia systemu informatycznego ma obowiązek:
   - zabezpieczyć ślady pozwalające na określenie przyczyny naruszenia systemu informatycznego,
   - przeanalizować i określić skutki naruszenia systemu informatycznego,
   - określić czynniki, które spowodowały naruszenie systemu informatycznego,
   - dokonać niezbędnych korekt w systemie informatycznym polegających na zabezpieczeniu systemu przed ponownym jego naruszeniem,
   - powiadomić o naruszeniu systemu informatycznego jego przyczynach i skutkach oraz podjętych działaniach korygujących system.

§ 9

1. Administrator prowadzi rejestr pracowników – użytkowników systemu informatycznego, zawierający:
   - imię i nazwisko pracownika,
   - stanowisko,
   - zakres, w jakim pracownik został dopuszczony do przetwarzania danych osobowych w systemie informatycznym,
   - datę wydania upoważnienia,
   - datę utraty upoważnienia,
   - indywidualny identyfikator pracownika.

2. System informatyczny powinien zapewnić odnotowanie:
   - daty wprowadzenia i modyfikacji danych osobowych,
   - identyfikatora użytkownika systemu wprowadzającego dane,
   - informację, komu, kiedy i w jakim zakresie dane zostały udostępnione,
   - żądanie zaprzestania przetwarzania danych po jego uwzględnieniu.

3. System informatyczny służący do przetwarzania danych osobowych musi pozwalać na udostępnienie tych danych na piśmie w formie powszechnie zrozumiałej.

§ 10

Zarządzenie wchodzi w życie z dniem podpisania.