ZARZĄDZENIE Nr 20/2018
Wójta Gminy Szczytniki
z dnia 20 czerwca 2018 r.

w sprawie: **wyznaczenia Inspektora Ochrony Danych w Urzędzie Gminy w Szczytnikach.**

Na podstawie art. 31 i art. 33 ust. 3 ustawy z 8 marca 1990 r. o samorządzie gminnym (tj. Dz. U. z 2018 r. poz. 994 z późn. zm.) oraz art. 37 ust. 1, lit.a rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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) **zarządza się, co następuje:**

§ 1. Wyznacza się Pana Dariusza Wawrzyniaka - pracownika tutejszego Urzędu, na Inspektora Ochrony Danych w Urzędzie Gminy w Szczytnikach.

§ 2. W załączniku do niniejszego zarządzenia ustala się ramowy zakres zadań Inspektora Ochrony Danych.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Marek Albrecht

Załącznik
do Zarządzenia Nr 20/2018
Wójta Gminy Szczytniki
z dnia 20 czerwca 2018 r.

RAMOWY ZAKRES ZADAŃ
INSPEKTORA OCHRONY DANYCH
w URZĘDZIE GMINY w SZCZYTNIKACH

1. Inspektor Ochrony Danych realizuje obowiązki zgodnie z wymaganiami obowiązującego prawa przy uwzględnieniu ryzyka i oceny skutków związanych z czynnościami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania;

2. Osoby, których dane są gromadzone i przetwarzane, mogą kontaktować się z Inspektorem Ochrony Danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy przepisów prawa powszechnie obowiązującego i aktów prawa wewnętrznego; (wniosek o realizację praw stanowi załącznik nr ..... do niniejszej Polityki);

3. Inspektor Ochrony Danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z przepisami prawa powszechnie obowiązującego i regulacjami wewnętrznymi;

4. Inspektor Ochrony Danych zobowiązany jest w szczególności do:
   1) informowania Administratora oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach spoczywających na nich na mocy powszechnie obowiązujących przepisów prawa oraz aktów prawa wewnętrznego w zakresie ochrony danych osobowych i doradzanie im w tej sprawie,

   2) nadzorowania i monitorowania przestrzegania przepisów prawa o ochronie danych oraz aktów prawa wewnętrznego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu Administratora i podmiotów trzecich uczestniczącego w operacjach przetwarzania oraz powiązanych z tym audytów,

   3) udziału w ocenie skutków dla ochrony danych zgodnie z art. 35 RODO oraz monitorowanie wykonania zaleceń opracowanych w wyniku wykonania oceny,

   4) współpracy z organem nadzorczym, pełnienia funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,

   5) weryfikacji zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie, minimum raz w roku sprawozdania dla Administratora,

   6) przygotowywania do końca grudnia każdego roku Planu sprawdzeń (audytów) na następny rok i przedstawienie go Administratorowi, a po akceptacji jego realizację; plan sprawdzeń jest określeniem harmonogramu weryfikacji systemu ochrony danych osobowych i w okresie pięciu lat sprawdzenia powinny łącznie objąć:

      a) zabezpieczenia: organizacyjne i techniczne zbiorów danych osobowych,

b) system informatyczny służący do przetwarzania danych osobowych,
c) kompletność zidentyfikowanych zbiorów danych osobowych,
d) przesłanki legalności przetwarzania danych osobowych,
e) przesłanki legalności przetwarzania danych szczególnie chronionych,
f) zakres i cel przetwarzania danych,
g) merytoryczną poprawność danych i ich adekwatność do celu przetwarzania,
h) obowiązek informacyjny,
i) profilowanie,
j) przekazywanie danych do państwa trzeciego, w tym do krajów spoza Unii Europejskiej,
k) powierzenie przetwarzania danych osobowych (w tym zakres i poprawność konstruowania umów powierzenia przetwarzania danych),
l) zgodność dokumentacji przetwarzania danych osobowych z obowiązującymi przepisami prawa powszechnie obowiązującego i stosowanymi w Jednostce Organizacyjnej zabezpieczeniami, technologiami, systemami, itp,

7) opracowania i aktualizowania Polityki Bezpieczeństwa Danych Osobowych oraz dokumentami związanymi z przetwarzaniem danych osobowych;

8) wspieranie administratora w realizacji przygotowywaniu odpowiedzi na żądania osób, których dane dotyczą, uzyskania od administratora potwierdzenia, czy przetwarzane dane osobowe jej dotyczące, a jeżeli ma to miejsce, uzyskanie dostępu do nich wraz z zakresem właściwych informacji o danych osobowych,

9) informowania o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania osób, które wystąpiły z takim żądaniem;

10) prowadzenia i aktualizacji rejestru czynności przetwarzania;

11) prowadzenia i aktualizacji rejestru naruszeń bezpieczeństwa, zgodnie ze wzorem wskazanym w załączniku nr ..... do Polityki Bezpieczeństwa Informacji;

12) przygotowania i przekazywania do podpisu do Administratora zgłaszania o naruszeniu ochrony danych osobowych do organu nadzorczego oraz zawiadamiania osoby, której dane dotyczą o naruszeniu ochrony danych osobowych – zgodnie z postanowieniami art. 33 i 34 RODO;

13) prowadzenia i aktualizacji rejestru umów powierzenia przetwarzania danych, zgodnie ze wzorem wskazanym w załączniku nr ..... do Polityki Bezpieczeństwa Informacji;

14) nadzorowania i monitorowania procesu profilowania (o ile taki ma miejsce);

15) opiniowania umów zawieranych z podmiotami trzecimi w zakresie ich zgodności z przepisami prawa powszechnie obowiązującego i wewnętrznego w zakresie ochrony danych osobowych;

16) nadzorowania i monitorowania realizacji obowiązku informacyjnego, zgodnie z wymogami RODO;

17) prowadzenia Rejestru zgłoszonych sprzeciwów dotyczących przetwarzania danych osobowych i wniosków o zaprzestanie lub ograniczenie przetwarzania danych;

18) informowanie Administratora o wystąpieniu incydentu;

19) przygotowania wzorów klauzul informacyjnych i umów powierzenia przetwarzania danych;

20) gromadzenia potwierdzenia (dotyczy formy papierowej) wywiązania się z obowiązku informacyjnego oraz weryfikacji prawidłowości gromadzenia potwierdzeń w systemach informatycznych;

21) prowadzenia ewidencji upoważnień do przetwarzania danych osobowych oraz dokumentacji związanej z udzieleniem upoważnień, zgodnie ze wzorem zawartym w załączniku nr ..... Do PBI;

22) przygotowywania upoważnień do przetwarzania danych osobowych zgodnie ze wzorem zawartym w załączniku nr ..... do PBI;

23) wykonania szacowania ryzyka i oceny skutków przed wprowadzeniem nowej technologii (np. nowego systemu informatycznego, w którym przetwarzane będą dane osobowe wraz z administratorem systemu i właścicielem zasobu;

5. Inspektor Ochrony Danych jest uprawniony szczególności do:
   1) wstępu do pomieszczeń, w których przetwarzane są dane osobowe,

   2) odbierania wyjaśnień od osób przetwarzających dane osobowe,

   3) dokumentowania ustaleń i dokonywania innych czynności niezbędnych do wykonania jego zadań wynikających z RODO, Ustawy, aktów prawa wewnętrznego i zakresu jego obowiązków/zakresu umowy o świadczenie usług;

   4) Szczegółowy zakres uprawnień Inspektora Ochrony Danych określa RODO i Ustawa.

WÓJT
Marek Albrecht